

Deli. PLNG is UNINTENDED

**United States Space Command
(USSPACECOM)**

Concept of Operations (CONOPS)

For

Computer Network Defense (CND)

Form SF298 Citation Data

Report Date ("DD MON YYYY") 01101999	Report Type N/A	Dates Covered (from... to) ("DD MON YYYY")
Title and Subtitle United States Space Command (USSPACECOM) Concept of Operations (CONOPS) For Computer Network Defense (CND)		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) United States Space Command (USSPACECOM)		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms "IATAC COLLECTION"		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 115		

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 074-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED	
	10/1/99	Report	
4. TITLE AND SUBTITLE United States Space Command (USSPACECOM) Concept of Operations (CONOPS) For Computer Network Defense (CND)		5. FUNDING NUMBERS	
6. AUTHOR(S) HQ USSPACECOM/J39			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060		10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES			
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A
13. ABSTRACT (Maximum 200 Words) This CONOPS explains the responsibilities articulated in the Implementation Plan (IPLAN) and identifies how USSPACECOM and the JTF-CND will execute the DOD CND mission. It does not replicate or replace the existing JTF-CND tactics, techniques and procedures (TTP). The CND CONOPS consists of measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. This complex mission area is dynamic and global in nature. It encompasses people, hardware, software and the networks that bind them together. The CND mission is executed in an environment characterized by the rapid movement of information that is vulnerable to incidents from anywhere, by anyone, at anytime. Within this mission area and environment, USSPACECOM is the military lead responsible for coordinating and directing the protection and defense of DOD computer networks and information systems.			
14. SUBJECT TERMS USSPACECOM,			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None

MEMORANDUM FOR DISTRIBUTION

8 Oct 99

FROM: USSPACECOMN3
250 S. Peterson Blvd Ste 116
Peterson AFB CO 80914-3040

SUBJECT: Approved USSPACECOM Concept of Operations for Computer Network Defense

1. The USSPACECOM Concept of Operations (CONOPS) for Computer Network Defense (CND) has been approved by USCINCSpace and is provided for your use. This CONOPS explains the responsibilities articulated in the Implementation Plan (IPLAN) and identifies how USSPACECOM and the JTF-CND will execute the DoD CND mission. It does not replicate or replace the existing JTF-CND tactics, techniques and procedures (TTP).
2. This document is derived from the tenets articulated in Joint Doctrine and will be successfully executed as a joint team through close coordination with numerous mission partners. It is a living document and as we gain more experience with the CND mission, we plan to incorporate lessons learned and republish the CND CONOPS in early calendar year 2000. We welcome your comments throughout the evolution of the CND mission. If you have questions or comments, please contact SPJ39C, Lt Col Joe Squatrito, DSN 692-6777, squatritoj@usspace.cas.spacecom.af.mil (text only) or on SIPRNET at squatritoj@netspot.usspace.spacecom.smil.mil. The CND CONOPS is available on SIPRNET at <http://www.usspace.spacecom.smil.mil/SJ5/CNDA/index.htm>.

//SIGNED//

THOMAS B. GOSLIN, JR.
Major General, USAF
Director of Operations

Attachment

1. USSPACECOM CND CONOPS, 1 Oct 99

DISTRIBUTION

HQ USSPACECOM/J1/J2/J3/J4/J5/J6/AN/PA/JA/
CMOC/CC
CJTF-CND
JIOC/CC
COMAFSPACECOM
COMNAVSPACECOM
COMARSPACECOM (Fwd)
JOINT STAFF/J2
JOINT STAFF/J3
JOINT STAFF/J5
JOINT STAFF/J6
USCENTCOMN3
USSTRATCOM/J3
USSOUTHCOMN3
USACOM/J3
USPACOM/J3
USSOCOM/J3
USEUCOM/J3
USTRANSCOM/J3
HQ NORAD/J3
NSA
DIA
NRO
USAF
USN
USA
USMC

EXECUTIVE SUMMARY

Subject to the authority and direction of the Secretary of Defense, USCINCSpace, in conjunction with the Joint Staff and appropriate CINCs, is assigned the responsibility as the military lead for Computer Network Defense (CND) and effective 1 October 2000, Computer Network Attack (CNA). In this capacity, USCINCSpace will coordinate and direct operations to protect and defend the computer systems and networks of the Defense Information Infrastructure (DII) or other vital national security interests, as directed, against computer network attacks and intrusions. On behalf of all CINCs, Services, and DoD Agencies (C/S/As), USCINCSpace will advocate for CND and CNA requirements, conduct CND and CNA operations, plan and develop national requirements for CND and CNA, and support other CINCs for CND and CNA.

The CND Concept of Operations (CONOPS) provides direction to the USSPACECOM staff, Space Operations Center (SPOC), and JTF-CND in executing the DoD CND mission. It is not intended to govern the entire DoD in CND mission execution. It does not govern or address the USSPACECOM internal IO/IA mission,

The CND CONOPS consists of measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. This complex mission area is dynamic and global in nature. It encompasses people, hardware, software and the networks that bind them together. The CND mission is executed in an environment characterized by the rapid movement of information that is vulnerable to incidents from anywhere, by anyone, at anytime. Within this mission area and environment, USSPACECOM is the military lead responsible for coordinating and directing the protection and defense of DoD computer networks and information systems.

USCINCSpace has approved the attached CND Concept of Operations. The CND CONOPS describes how USSPACECOM and its components will execute the CND mission. Furthermore, it describes how USSPACECOM will seek to influence and foster DoD policy and initiatives that provide common operating procedures and standards for accomplishing timely and effective CND. This CONOPS is composed of four major sections.

Section 1, Introduces the CND mission CONOPS with a purpose for the document, reviews the authority for CONOPS publication and describes the USSPACECOM focus and mission objectives detailed in subsequent sections. In addition, this section provides background information on the computer network intrusion/attack threat to national security and a brief overview of the operating environment of the Defense Information Infrastructure (DII).

Section 2, describes the CND mission, USCINCSpace commander's intent, vision and strategy. Command relationships and authorities are reviewed and a list of USSPACECOM priorities and tasks is provided. Finally, roles and responsibilities are reviewed with discussion on inherent shared responsibilities for the global CND mission.

Section 3 describes USSPACECOM CND mission operations. It specifically describes the interrelationship and processes used by USCINCSpace, HQ Joint Task Force-Computer Network Defense (JTF-CND), and USSPACECOM staff elements to execute the CND mission. The section emphasizes the USSPACECOM approach to mission operations including daily activity reporting, training, and exercises. Operations support requests are discussed, as well as USSPACECOM plans to conduct deliberate planning and Course Of Action development.

Section 4, Support to Operations describes how Headquarters USSPACECOM staff elements will support CND mission operations. Functional areas discussed include legal; manpower and personnel; intelligence; logistics; plans and policy; command, control and communications; and public affairs.

Planning and execution of the Computer Network Defense (CND) mission, as described in this Concept of Operations (CONOPS) will be predicated on, and commensurate with, the approval of requisite funding and manpower as delineated in the current Program Objective Memorandum (POM) and the CND Implementation Plan.

As experience with CND mission increases, USSPACECOM/J3 will periodically review and update the CND CONOPS. All comments should be addressed to USSPACECOM/J39, 250 S. Peterson Blvd, Suite 116, Peterson AFB, Colorado 80914-3090.

HEADQUARTERS, U.S. SPACE COMMAND
250 S Peterson Blvd, Suite 116
Peterson AFB, CO 80914-3010
1 September 1999

USSPACECOM Computer Network Defense (CND) Concept of Operations (CONOPS)

EXECUTIVE SUMMARY..... ii

TABLE OF CONTENTS..... iii

1 .0. INTRODUCTION	1-1
1.1. Purpose	1-1
1.2. Authority	1-1
1.3. Focus and Objectives	1-1
1.4. Background Information	1-2
2.0. MISSION	2-1
2.1. USCINCSpace Intentions.	2-1
2.2. JTF-CND Mission...	2-1
2.3. USCINCSpace Commander's Intent..	2-1
2.4. USCINCSpace Vision..	2-2
2.5. USCINCSpace Strategy..	2-2
2.6. Command Relationships..	2-2
2.7. USCINCSpace Priorities and Tasks	2-4
2.8. Roles and Responsibilities	2-6
3.0. OPERATIONS	3-1
3.1. USCINCSpace's CND Operations	3-1
3.2. USSPACECOM CND Operational Relationships	3-12
3.3. Commanders Critical Items of Information	3-14
3.4. USCINCSpace Assessment Process..	3-20
3.5. Deliberate Planning	3-22
3.6. Crisis Action Planning	3-23
3.7. Support Requests..	3-24
3.8. Red Team Resources and Support.	3-26
3.9. Exercises	3-26
3.10. Global Partnering..	3-31
4.0. SUPPORT TO OPERATIONS	4-1
4.1. Legal	4-1
4.2. Manpower and Personnel	4-1
4.3 Intelligence Support To Operations	4-1
4.4. Logistics	4-2
4.5. Plans and Policy	4-2
4.6. Command, Control and Communications	4-4

4.7. Space Operations Support Branch	4-5
4.8. NORAD-SPACECOM Operations Branch	4-6
4.9. Public Affairs..	4-6

List of Figures

Fig 1-1. Defense Information Infrastructure	I-3
Fig 2-1. Command Relationships..	2-3
Fig 2-2. USCINCSpace Initial Priorities for Protecting the DII..	2-5
Fig 2-3. USPACECOM CND Relations..	2-7
Fig 2-4. Shared CND Responsibilities	2-8
Fig 3-1. USCINCSpace's Process Model for CND..	3-1
Fig 3-2. CND Reporting	3-9
Fig 3-3. USSPACECOM CND Relationships..	3-12
Fig 3-4. USCINCSpace Assessment Process	3-21
Fig 3-5. USCINCSpace Training and Education Initiatives	3-25
Fig 3-6. Exercise Assessment Process	3-30
Fig C-1. CND Taxonomy..	C-2

List of Tables

Table 3-1. CND Process and Elements Overview	3-2
Table 3-2. Protection of Computer Information Environment	3-2
Table 3-3. Policy Activities In CND Protection	3-3
Table 3-4. Capabilities and Procedures In CND Protection	3-5
Table 3-5. Defensive Operations In CND Protection	3-7
Table 3-6. Detection of Attacks and Intrusions	3-8
Table 3-7. Restoration after Attack or Intrusion	3-I 0
Table 3-8. Response to Attacks and Intrusions	3-I 1
Table 3-9. Notional Apollo CND Planning Timelines..	3-28
Table A-1. Minimum Position Distribution	A-1

APPENDICES

- A. Minimum Mission Resources
- B. References
- C. Glossary of Terms and Acronyms

ANNEXES

1. USSPACECOM Internal Organization and Tasks
2. USSPACECOM Intelligence Concepts For Support To CND Operations

DISTRIBUTION LIST

For Action

HQ USSPACECOM/J1/J2/J3/J4/J5/J6/JS/JA/PA
Commander Joint Task Force-CND

For Information

Joint Staff /J-39/J-6K
Director of Operations, US Atlantic Command
Director of Operations, US Central Command
Director of Operations, US European Command
Director of Operations, **US** Pacific Command
Director of Operations, US Southern Command
Director of Operations, US Special Operations Command
Director of Operations, US Strategic Command
Director of Operations, US Transportation Command
Director of Operations, US Forces Korea
Chief of Staff, US Army
Chief of Naval Operations
Chief of Staff, US Air Force
Commandant of the Marine Corps
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
Director, National Security Agency
Director, Central Intelligence Agency
Director, National Reconnaissance Office
Director, National Imagery and Mapping Agency
Director, Defense Logistics Agency
Commander, Air Force Space Command
Commander, Army Space Command
Commander, Navy Space Command

1 .O. Introduction. This section provides the purpose of the CND CONOPS, reviews the authority for CONOPS publication and describes the USSPACECOM focus and objectives for the CND mission. In addition, this section provides background information on the threat to U.S. national security and computer networks and a brief overview of the operating environment of the Defense Information Infrastructure (DII).

1 .1. Purpose. The 1999 Unified Command Plan (UCP) assigns the Commander in Chief, United States Space Command (USCINCSpace) as the military lead for CND and Computer Network Attack (CNA) of DII. USCINCSpace will assume responsibility for CND beginning 1 October 1999 and for CNA on 1 October 2000. This CONOPS describes how USCINCSpace will execute responsibilities for the CND mission. A separate CNA CONOPS will be published in 2000 detailing USSPACECOM execution of the CNA mission.

1.2. Authority. The CND CONOPS will be approved by USCINCSpace. Upon approval, the CND CONOPS provides overarching guidance and direction to HQ USSPACECOM, the USSPACECOM Space Operations Center (SPOC), and the JTF-CND for execution of the DoD CND mission. As experience with the CND mission increases, USSPACECOMN3 will periodically review and update the CND CONOPS. All comments should be addressed to USSPACECOM/J39, 250 S. Peterson Blvd, Suite 116, Peterson AFB, Colorado 80914-3090.

1.3. Focus and Objectives. The focus of this document is on the mission interface between HQ USSPACECOM and the JTF-CND; and the actions required by HQ USSPACECOM to support the CND mission and the JTF-CND.

1.3.1. This CONOPS achieves three objectives:

- a. Describes the operational interface between HQ USSPACECOM and JTF-CND to accomplish the CND mission.
- b. Describes and clarifies internal HQ USSPACECOM staff responsibilities required to execute and support the CND mission.
- c. Describes external relationships between USCINCSpace and CINCs/Services/DoD Agencies (C/S/A); and the desired relationships required between USSPACECOM and external agencies and industry to provide effective CND.

1.3.2. This CONOPS does not address internal JTF-CND processes such as monitoring, evaluating or characterizing events or event/incident reporting by the service Computer Emergency Response Team/Computer Information Response Team (CERT/CIRT) activities. For information concerning detailed JTF-CND mission operations functions, refer to the Concept of Operations for the Joint Task Force-Computer Network Defense [see: <http://www.jtfcnd.ia.smil.mil/>].

1.4. Background Information.

1.4.1. Threat. The October 1998 National Security Strategy of the United States recognized the need to enhance U.S. security due to the diverse threats to our computer network systems. These threats range from regional or state-centered threats to emerging transnational threats. Another significant threat to national security arises from foreign intelligence collection activities involving intrusion into DoD computer networks.

1.4.1.1. National and Transnational Threats. Threats to U.S. national information infrastructure range from cyber-crime to unambiguous strategic information attack (via the global information network). Unlawful intrusions and cyber-attack of our information networks could originate from terrorists, criminal groups, or organized states with hostile intent towards the United States.

1.4.1.2. Foreign Intelligence Collection. The U.S. also faces an increased threat from foreign intelligence collection activities. Some foreign intelligence services are rapidly employing new technologies and innovative methods to gain access to sensitive information by penetrating computer networks and systems.

1.4.2. Operating Environment

1.4.2.1. Defense Information Infrastructure (DII). The DII consists of shared or interconnected computers, communications, data applications, security, people, training, and other support structures serving the DoD's need for local, national, and worldwide information. The DII is part of the National Information Infrastructure (NII) and the larger Global Information Infrastructure (GII). The structure and nature of global DII computer network operations provides US war-fighting forces with tremendous advantages to plan and execute missions to meet our national security objectives. An operationally ready and secure DII enables U.S. information superiority.

Information Superiority

The capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same.

Joint Vision 2010

USSPACECOM CND Mission

Protect and Defend the DII

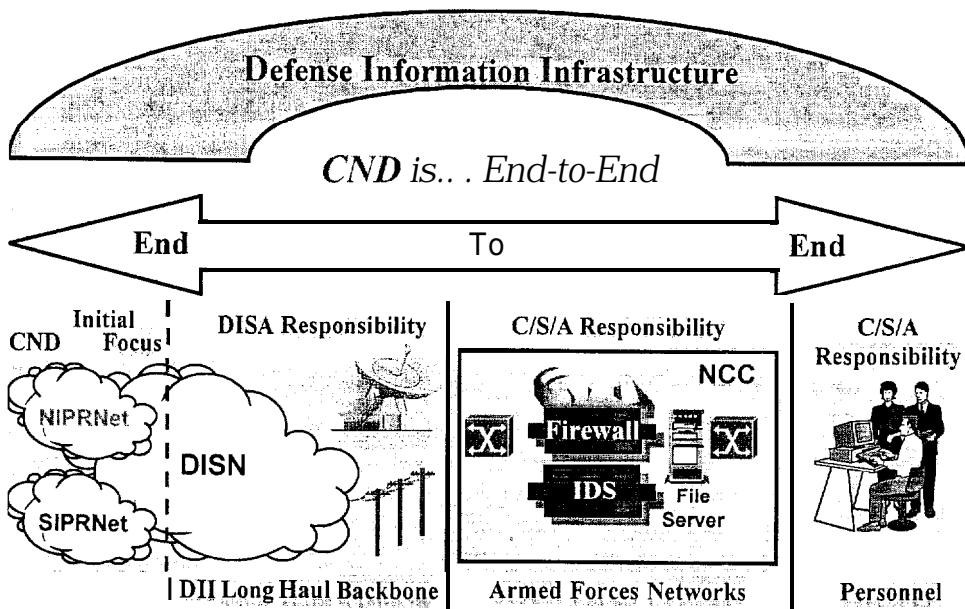


Figure I-I Defense Information Infrastructure (DII)

1.4.2.2. Shared Operational Risk. (Ref Figure I-I). While the DII enables US information superiority, the global inter-dependent nature of the DII also carries increasing levels of shared operational risks for all war-fighters and supporting activities. The role of USCINCSpace is to protect the DII so that the C/S/As can develop, coordinate, and execute plans to protect their individual AORs. In this process, each of the C/S/As must be aware that an intrusion (or confirmed attack) on a computer network in one region of the world may impact operations in another area. Therefore, CND is a shared responsibility. It is essential that USCINCSpace develop and maintain valid concepts, processes and capabilities to warn, protect and defend computer networks within the DII. USCINCSpace's initial focus will be to protect SIPRNET and NIPRNET but will support other networks as required (ref figure 2-2). In the final analysis, CND is an end-to-end, integrated and coordinated effort that includes training, certification, computer systems, networks, detection systems and interconnected communication links.

1.4.2.3. Future Network Systems -- Global Networked Information Enterprise (GNIE). The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) envisions a larger, more powerful DoD computer network capability beyond the DII, known as the GNIE. During planning and development of the GNIE, USCINCSpace will advocate CND operational concepts, as appropriate.

2.0. Mission. Subject to the authority and direction of the Secretary of Defense, USCINCSpace, in conjunction with the Joint Staff and appropriate CINCs, is assigned the responsibility as the military lead for Computer Network Defense (CND) and effective 1 October 2000, Computer Network Attack (CNA). In this capacity, USCINCSpace will coordinate and direct operations to protect and defend the computer systems and networks of the Defense Information Infrastructure (DII) or other vital national security interests, as directed, against computer network attacks and intrusions. On behalf of all CINCs, Services, and DoD Agencies (C/S/As), USCINCSpace will advocate for CND and CNA requirements, conduct CND and CNA operations, plan and develop national requirements for CND and CNA, and support other CINCs for CND and CNA.

2.1. Supporting and Supported CINC.

2.1 .1. Supporting CINC. USCINCSpace intends to provide integrated CND, CNA, and space support to Joint Force Commanders (JFCs). USCINCSpace will also provide operational advocacy for CND policy, doctrine, education and mission-level requirements involving operational CND matters. This advocacy role will be conducted on behalf of all regional and functional CINCs. USCINCSpace will coordinate with the other **CINCs**, the Intelligence Community (IC), and DoD agencies on all matters associated with execution of CND mission responsibilities.

2.1.2. Supported CINC. Our prevalent role will be as a supporting CINC, protecting and defending computer networks and systems vital to JTF operations. However, during a large-scale attack on the DII or other critical situations, USCINCSpace may also serve as a supported CINC. In the event of such a significant attack, USCINCSpace will coordinate and direct specific protect and response actions, and coordinate restoration actions across the DoD operations. Every effort will be made to deconflict and minimize the impact on DoD operations. Designation as a supported CINC will be made by the CJCS through the normal JOPES process.

2.2. JTF-CND Mission. Subject to the authority and direction of USCINCSpace JTF-CND will, in conjunction with the C/S/A, be responsible for coordinating and directing the defense of DoD computer systems and networks. This mission includes the coordination of DoD defensive actions with non-DoD government agencies and appropriate private organizations.

2.3. USCINCSpace Commanders Intent. USCINCSpace intends to:

- a. Lead DoD and CND mission partners to protect and defend the DII
- b. Unify mission partners and existing capabilities
- c. Provide operational focus to CND efforts
- d. Standardize levels of CND protection for DoD networks
- e. Establish a rapid and effective response process
- f. Advocate for CND policy, capabilities, requirements, and education and training

2.4. USCINCSpace Vision. USCINCSpace has adopted the following preliminary statements outlining the vision for CND and CNA. The preliminary CNA vision is provided in this document to demonstrate the balance of focus and perspective as the mission is adjusted in 2000 for CNA.

2.4.1. For the CND mission, USCINCSpace vision is to provide "Coordinated joint, combined, civil, and commercial efforts to protect/defend computer networks vital to national security."

2.4.2. For the CNA mission, USCINCSpace vision is "Synchronized joint operations to gain and exploit information superiority and denial of adversary ability to do the same."

2.5. USCINCSpace Strategy. As the military lead for CND, USCINCSpace will leverage existing CND efforts and programs by integrating operations, planning, policy, requirements, and personnel actions, and forge mission partnerships with the diverse array of existing CND activities. Potential mission partners include DoD agencies, the intelligence community, other US government agencies, industry, and US allies associated with the CND mission. These partnerships are appropriate and necessary due to the common interests of the DII. Furthermore, USCINCSpace will foster a positive, constructive atmosphere to further enhance shared situational awareness of computer network defense measures.

2.5.1. Layered Network Defense. USCINCSpace advocates a layered network defense through mutual support and dialogue for computer network defense matters. The concept for layered defense is as follows:

2.5.1.1. Empowerment of commanders at all levels to protect and defend their networks.

2.5.1.2. Integration/coordination of actions across DoD ensuring they are mutually supportive. This may include coordinated responses: passive (blocking, detecting, reporting); active (pursuit, LEA, CI); and, offensive (developing COAs for NCA approval) actions.

2.5.1.3. Focus on protection and support of military operations.

2.6. Command Relationships. Figure 2-I provides an overview of command relationships between USCINCSpace, the JTF-CND, Unified Commands, Services, and Agencies. The following command relationships are effective 1 Oct 1999.

Command Relationships

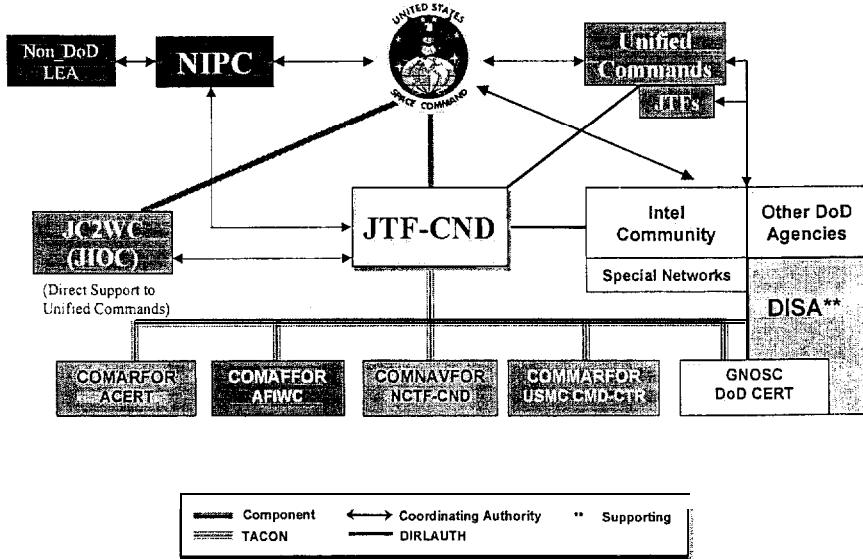


Figure 2-1 Command Relationships

2.6.1. USSPACECOM Authorities

2.6.1.1. USCINCSpace exercises Combatant Command (COCOM) authority for JTF-CND.

2.6.1.2. USCINCSpace exercises coordinating authority with all CINCs, Services and DoD Agencies (C/S/A) for the assigned CND mission, as defined by Joint Publication (JP) I-02.

2.6.1.3. USCINCSpace plans for and directs the execution of the DoD CND mission. This includes the operational advocacy for CND policy and requirements for Joint Chiefs of Staff approval. This also includes CND mission coordination, integration, and advocacy of Rules of Engagement (ROE) or changes to ROE.

2.6.1.4. Effective 1 October 1999, the Secretary of Defense has delegated approval authority to USCINCSpace for DoD INFOCON changes.

2.6.2. JTF-CND Authorities

2.6.2.1. Commander, JTF-CND (CJTF-CND), will exercise Tactical Control (TACON) authority over assigned Service CND components (e.g., CERTs/CIRTS); and three activities organized by the Defense Information Systems Agency (DISA): the DoD CERT; the Global Network Operations Security Center (GNOSC); and, the Joint Web Risk Assessment Cell (JWRAC).

2.6.2.2. CJTF-CND directs and conducts CND mission operations as required to protect and defend the DII. This authority pertains to all operational actions that do not require

USCINCSpace involvement, as explained in par. 3.2.5. In those instances requiring USCINCSpace involvement, CJTF will recommend courses of action, options, and technical solutions. Upon USCINCSpace approval, JTF-CND will direct execution of approved actions to all C/SAs for implementation.

2.6.2.3. JTF-CND is authorized Direct Liaison Authorized (DIRLAUTH) with all C/S/A, non-DoD CERTS and LEAs to exchange information in order to perform assigned mission and tasks. The JTF-CND is also authorized direct coordinating authority with the Joint Information Operations Center (JIOC).

2.7. USCINCSpace Priorities and Tasks.

2.7.1. Mission Priorities. (Ref figure 2-2) USCINCSpace approved initial priorities for planning and execution of the CND mission as follows:

- a. Protect and defend the Defense Information System Network (DISN), including the Sensitive but Unclassified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET). Figure 2-1 graphically shows the relationship of the SIPRNET and NIPRNET to other computer network systems.
- b. Protect and defend critical Command and Control (C2) systems that use the DISN for transport (i.e., the Global Command and Control System, Global Combat Support System, and Defense Messaging System).
- c. Protect and defend SIPRNET common user systems (e-mail and web services). This includes intelligence sub-networks on the SIPRNET and other C2 systems on the DISN, and other systems and networks that the C/S/A and the intelligence community own and operate.
- d. Protect and defend NIPRNET mission support systems. These generally include administrative e-mail services, web services, research and development systems and logistics and payroll systems.

USCINCSpace Initial CND Focus

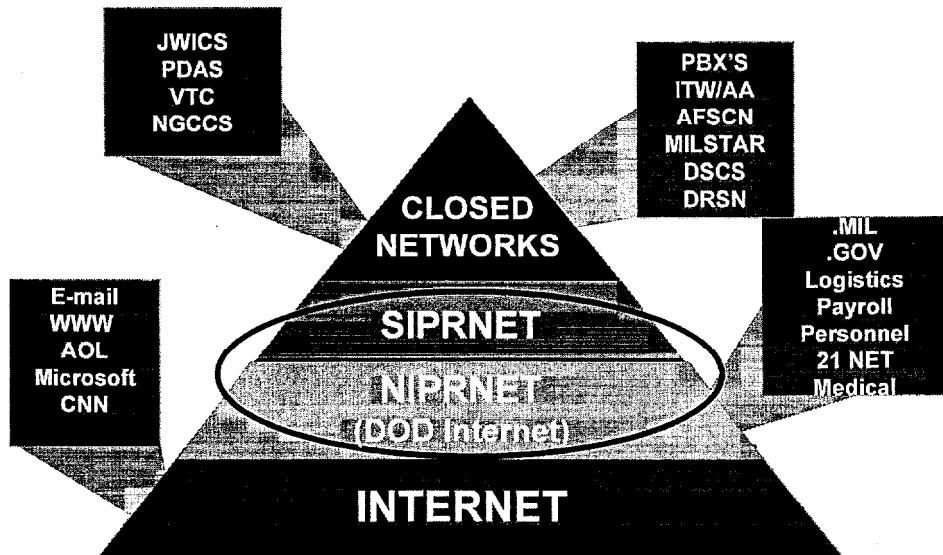


FIGURE 2-2 USCINCSpace Initial Priorities for Protecting the DII.

2.7.2. Prioritized Tasks. USCINCSpace approved fourteen prioritized tasks for the CND mission beginning 1 Oct 99.

2.7.2.1. As the mission begins with limited resources available, the following four tasks will receive initial priority:

- a. Monitor/Support Real World CND mission operations. Coordinate CND actions with regional CINCs, Services, OSD, Joint Staff, DoD Agencies, LE, CI, IC and others as required, to support the operational execution of the mission
- b. Prepare for Y2K – Predictive analysis/Contingency Plan for responding to potential hostile “Y2K disguised” events
- c. Prepare for CND Exercise (Apollo CND in spring 2000)
- d. Review/advocate CND Policy / Doctrine / ROE issues

2.7.2.2. When more CND resources become available, USCINCSpace will pursue these additional 10 tasks:

- a. Provide Intelligence Support to Operations-Detailed development of EEIs, PIRs, I&W, Collection Management Plans, and Threat Assessments

- b. Conduct Deliberate Planning – coordination into other CINC OPLANS, CONPLANS
- c. Develop Unified Instructions (UI), INFOCON determination, reporting processes, coordinate Joint Tactics, Techniques and Procedures (JTTP)
- d. Advocate JMRR and readiness indicator development
- e. Provide operational requirements development and advocacy
- f. Advocate technical Support for JTF-CND
- g. Advocate for training, education, modeling/simulation, exercise coordination (including Red Team activities)
- h. Establish backup JTF-CND operations center
- i. Monitor DII components to identify additional USCINCSpace protection role
- j. Coordinate staff assistance visits – monitor / evaluate valid DII configuration compliance (recurring assessment of DoD computer network vulnerabilities)

2.8. Roles and Responsibilities.

2.8.1. USSPACECOM will use the normal Unified Command to JTF relationship model to delineate roles and responsibilities between **HQ USSPACECOM** and the JTF-CND. For example, HQ USCENTCOM coordinates mission support and guidance (policy, ROE, plans, requirements, etc.) and integrates required support for their operations across other CINCs, Services, DoD agencies, the Intel Community, and many others. JTF-SWA executes the mission and guidance provided by HQ USCENTCOM. Likewise, HQ USSPACECOM will focus on policy, process, mission-coordination, integration-type roles, while the JTF-CND will focus on operational mission execution. HQ USSPACECOM will interact with a variety of mission partners-other CINCs, Services, JS, OSD, DoD agencies, DISA, the Intelligence Community, NSA (for DIO support), law enforcement agencies, NIPC, industry, and others. This coordination will integrate support across all these partners to continuously improve the DoD's CND process and support the JTF-CND. These process-oriented activities will complement the JTF-CND's mission execution responsibilities. USCINCSpace's focus will be global in nature ensuring the overall security and integrity of the DII. The C/SAs will retain responsibility for CND operations within their AORs.

2.8.1.1. The JTF-CND will execute the DoD CND mission. Its focus will be more procedural and operational, requiring close coordination across the community described above, but at a lower level. The JTF-CND will provide inputs to HQ USSPACECOM for policy, planning, ROE, requirements, and mission processes. But, their primary focus will be on the daily execution of the DoD CND mission-just as JTF-SWA's focus is on the daily execution of combat operations.

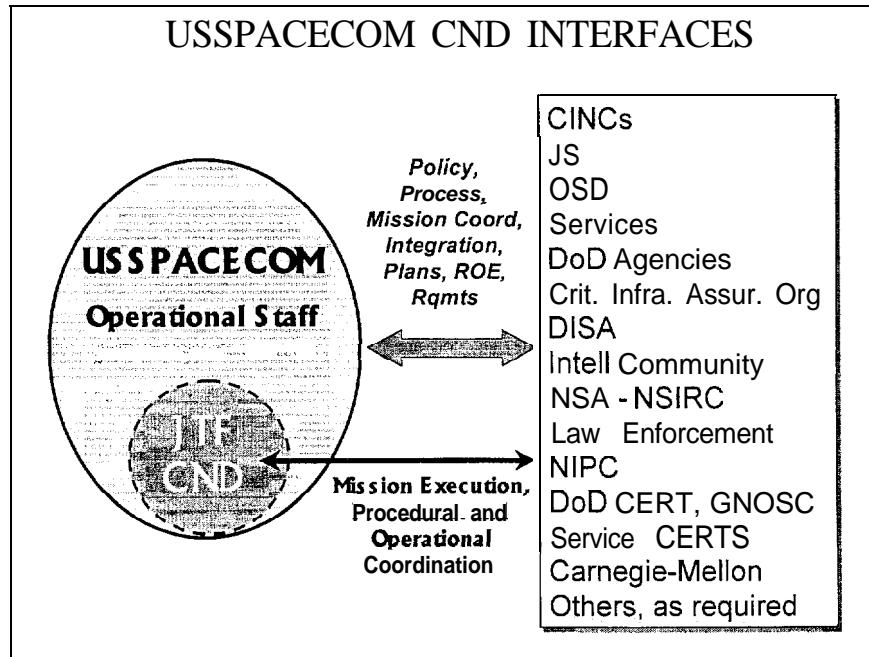


Figure 2-3 USSPACECOM CND Relations

2.8.1.2. USCINCSpace, through the USSPACECOMN3, will provide strategic guidance and direction to the Commander, JTF-CND through mission-type orders. The USSPACECOM/J2, J5, and J6 will provide support as described later in this document.

2.8.1.3. USCINCSpace will not assume regional/functional CINC responsibilities to maintain computer network defense and information assurance functions within their area of responsibility. USCINCSpace will not task-organize Service and DoD agency CERT/CIRT activities; and will not POM for DoD-wide CERT capabilities. This responsibility remains with the Services. USCINCSpace will advocate for mission-level requirements through the preparation and review of Mission Need Statements (MNS), Capstone Requirements Documents (CRDs) and Service Operations Requirements Documents (ORDs). However, USCINCSpace will not engineer, develop or acquire CND capabilities.

2.8.2. CINCs/Services/DoD Agencies (C/S/A) Roles and Responsibilities. All CINCs, Services and Agencies must continue to fulfill responsibilities to provide information assurance (IA) functions. Commanders at all levels retain authority to direct Information Conditions (INFOCON) to protect mission, life and property. Furthermore, all CINCs will continue to plan and execute information operations (IO) in accordance with established joint doctrine.

2.8.3. Shared CND Responsibilities. (Ref figure 2-4) Responsibility for the operational integrity of the DII carries shared operational risk. USCINCSpace will share responsibility for CND and integrity of the DII as shown below.

Shared CND Responsibilities

USSPACECOM:	OTHER CINCS:
<ul style="list-style-type: none">• Provide Global CND I&W• Provide Global CND Attack Assessment<ul style="list-style-type: none">– Correlate events across DOD– Determine mission impacts– Provide warnings, advisories• Integrate , Coord, Direct Responses<ul style="list-style-type: none">– Lead DOD response/recovery efforts• Develop OPlans, Annexes• Incorporate CND Into Joint Exercises• Facilitate Policy, Doctrine Development• Advocate DOD Mission-level Requirements	<ul style="list-style-type: none">• Provide Regional Attack Assessment<ul style="list-style-type: none">– Determine impacts on Force Structure and Mission– Provide Regional /Allied I&W• Integrate , Coord, Direct Own Responses<ul style="list-style-type: none">– Integrate DOD and Allied response/recovery efforts• Develop OPlans, Annexes• Incorporate CND Into Joint Exercises• Provide inputs and coordination on DOD Mission-level Requirements

Figure 2-4 Shared CND Responsibilities

2.8.4. Course of Action (COA) Development – Roles and Responsibilities. The JTF-CND and USCINCSpace, in coordination with C/S/As, will develop COAs for response to computer network incidents that involve or affect more than one C/S/A. The COAs will include the full spectrum of potential response actions from passive and active defense activities towards more offensive measures of defensive network operations (electronic and/or physical). (Ref 3.5.3. section 3, “Operations” for more detail).

2.8.4.1. For Passive Defense actions, JTF-CND will coordinate technical solutions and develop COA and recommendations, if required, for USCINCSpace decision. USSPACECOM/J36/J39 will monitor the world situation and national security objectives, and assist with CINC-level coordination with other CINC/Services/Agencies. J39/J36 will coordinate direction of strategic guidance, i.e., intent, objectives, etc., with JTF-CND.

2.8.4.2. For Active Defense actions against domestic perpetrators, DoD Law Enforcement Agencies (LEA) will lead DoD's COA development and recommendations. USSPACECOM/ J36/J39 will monitor national security concerns involved in the LEA activities and develop and coordinate applicable planning inputs for the LEA COA's. JTF-CND will provide technical advice and recommendations to USSPACECOM and assist LEA efforts as required. JTF-CND will deconflict passive defense activities and active defense activities.

2.8.4.3. For Defensive Network Operations, USCINCSpace will lead efforts to promulgate CND policy and coordinate operations. USCINCSpace will also conduct CND exercises. USCINCSpace will lead development, coordination, and execution of offensive COAs in response to specific threats to DoD networks and systems. Offensive response action may include diplomatic, economic, physical attack (kinetic),

or other actions (e.g., computer network attack options). USCINCSpace will coordinate with the JTF-CND to deconflict COAs with other defensive operations. USCINCSpace will also deconflict these response actions with the IC and offensive operations. After October 2000, USCINCSpace will be responsible for planning, coordinating, deconflicting, and executing DoD CNA options. All options will be coordinated with the designated supported CINC.

3.0. OPERATIONS

3.1. USCINCSpace's CND Operations. This section describes how USCINCSpace will defend computer networks on the DII from disruption, denial, degradation, or destruction. The USCINCSpace strategy is to employ a layered defense consisting of procedures, processes, and people to deter, contain, and negate attacks or intrusions. The strategy is executed through centralized coordination and, planning, and decentralized execution of the CND mission by the JTF-CND and other C/S/As as appropriate. The USSPACECOM staff provides planning, analyzes intelligence and threats, and coordinates activities throughout this process. The USSPACECOM model for CND is adapted from the Defensive Information Operations Process, outlined in CJCSI 6510.01B, and is illustrated in Figure 3-1 below. The model is based on four interrelated processes: 1) protection, 2) detection, 3) restoration, and 4) response.

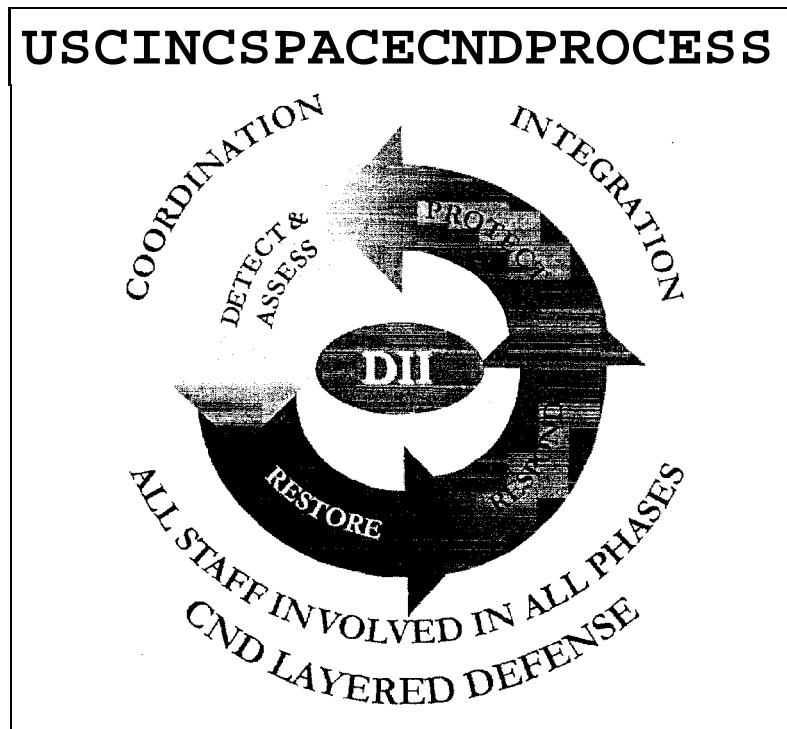


Figure 3-1. USCINCSpace's Process Model for CND

3.1 .1. Table 3-1, on the following page, is an overview of the Defensive Information Operations (DIO) process and the elements that comprise it, as described in CJCSI 6510.1 B. CND is comprised of activities from each of the four interrelated processes described in table 3-1. USCINCSpace responsibilities vary across the elements, from supporting and advocating to leading and directing. The tables and paragraphs that follow table 3-1 describe USCINCSpace relationships for each of the elements in the DIO process.

Overview of DIO Process and Elements	
<p>USCINCSpace CND PROCESS</p> <p>DIA</p> <p>COORDINATION INTELLIGENCE ASSESSMENT INTEGRATION</p> <p>ALL STAFF INVOLVED IN ALL PHASES CND LAYERED DEFENSE</p>	II Detect & Assess <ul style="list-style-type: none"> • Computer Network System Development • Providers/Administrators • Users • Law Enforcement • Intelligence/Counter Intelligence • Reporting III Restore <ul style="list-style-type: none"> • Backup Redundant Links • Inventory Tools and Techniques • Automated Decision Support • Restoration Assistance • Post-Attack Analysis IV Respond <ul style="list-style-type: none"> • Law Enforcement • Economic Sanctions • Diplomatic Actions • Military Force
I Protect <ul style="list-style-type: none"> • Policy <ul style="list-style-type: none"> -- Influence Policy Forums • Capabilities and Procedures Activities <ul style="list-style-type: none"> -- Information Assurance <ul style="list-style-type: none"> --- INFOSEC, COMPUSEC, COMSEC --- Education, Training and Awareness --- Intelligence --- Counter Intelligence --- Risk Management --- Vulnerability Analysis and Assistance --- Vulnerability Assessment -- Defensive Operations Activities <ul style="list-style-type: none"> --- Deterrent CND Capabilities --- CNA --- Other Military Operations 	(Derived from CJCSI 6510.1 B)

Table 3-1 Defensive Information Operations

3.1.2. **Protect.** Information protection is vital to the military's ability to conduct operations, and is applicable to virtually any medium through which information is conveyed. Protection of the information environment involves key activities in three areas: 1) Policy, 2) Capabilities and Procedures, and 3) Defensive Operations (Reference Table 3-2.) As the DoD military lead for the CND mission, USCINCSpace will execute operational responsibilities in all three areas for protection of information.

Protection Areas	USCINCSpace Roles and Responsibilities
Policies	Support and provide operational advocacy to national defense policy forums on issues involving protection of computer networks and systems.
Capabilities and Procedures	Advocate for actions that protect DoD computer networks and systems against attack/intrusion. When required, take actions to counter threats to DoD computer networks and system.
Defensive Operations	Conduct CND/A operations to deter attack/intrusions on DoD computer networks and systems. When deterrence fails, provide capabilities and COAs to defeat specific threats to DoD computer networks and systems.

Table 3-2. Protection of Computer Information Environment

3.1.2.1. Policy (Ref Table 3-3). USCINCSpace will support national defense forums as appropriate and provide operational advocacy on issues involving CND operations. This will include interaction with OSD, the JCS, and the C/S/As. USCINCSpace will also interact with non-DoD government and law enforcement agencies, the commercial sector, and allies and foreign governments (through the regional CINCs) in order to strengthen lines of communication and establish partnering initiatives for effective CND execution.

<u>Policy Activities</u>	<u>USCINCSpace Roles and Responsibilities</u>
Influence Policy Forums	<ul style="list-style-type: none"> - Interact with JCS and SECDEF. Provide a center of excellence for CND issues, policies, and doctrine. Advocate for new and/or revisions to current policy and doctrine. - Interact with DoD C/S/As. Provide a center of excellence for understanding and resolving CND issues, policies, and doctrine. Facilitate understanding and education of new or revised CND policy and doctrine. Understand and advocate for resolution of specific C/S/A CND issues and problems, - Interact with non-DoD Government/LEA /Agencies. Establish partnerships and strengthen lines of communications with applicable organizations that enhance effective DoD CND execution. Liaison and advocate issues, policies, and applicable doctrine Associated with mutual protection and inherent mission accomplishment. - Interact with Commercial and Civil Sector. Establish partnerships and strengthen lines of communications with applicable organizations that enhance effective DoD CND execution. Liaison and advocate issues, policies, and applicable doctrine associated with mutual protection, - Interact with Allies/Foreign Governments. Support regional and functional CINCs with establishing partnerships and strengthening lines of communications with foreign entities in their AORs that enhance effective CND execution.

Table 3-3. Policy Activities in CND Protection

3.1.2.2. Capabilities and Procedures (Reference Table 3-4). USCINCSpace will advocate for common CND capabilities and procedures that contribute directly to the protection of DoD computer networks and information security (INFOSEC).

<u>Capabilities and Procedures Activities</u>	<u>USCINCSpace Roles and Responsibilities</u>
Information Assurance - INFOSEC -- COMPUSEC -- COMSEC	- Advocate policy and capabilities that protect and defend information and information systems by ensuring availability, integrity, identification and authentication, confidentiality, non-repudiation. - Advocate capabilities that allow the ability to detect, document, and counter unauthorized access or modification of information - Advocate for measures and controls that ensure confidentiality, integrity and availability of information systems - Advocate measures to deny unauthorized persons information derived from telecommunications and ensure authenticity.
Education, Training, and Awareness	- Advocate CND education, training, exercises, and awareness programs. Facilitate implementation through DoD and Service schools, hosting conferences, etc.
Intelligence	- Develop a CND I&W center of excellence to provide I&W of attacks/intrusions on the DII computers and systems. - Support JTF-CND in leveraging intelligence assets, deconflicting, and dissemination of I&W information. - Correlate, deconflict, and fuse other mission related intelligence with CND incidents.
Counter Intelligence	- Advocate for policy and doctrine that strengthens the ability of CI assets to provide I&W, and pursuit of intruders/attackers for attribution. - Maintain awareness of CI efforts for the purpose of deconflicting those efforts from other CND activities. - Spearhead efforts to establish of MOAs with DoD and non-DoD LEAs for sharing and deconflicting information and activities impacting CND.

Risk Management	<ul style="list-style-type: none"> - Support the JTF-CND and, if required, direct actions for implementing CND countermeasures. - Advocate policy and standards that minimize/mitigate risk to and enhance protection of the DII.
Vulnerability Analysis and Assistance	<ul style="list-style-type: none"> - Coordinate and deconflict Red Team activities. - Provide “trusted agent” to deconflict analysis/assistance activities with current operations.
Vulnerability Assessment	<ul style="list-style-type: none"> - Monitor DoD vulnerability assessments in order to ensure high levels of operational readiness and integrity of DoD computer network operations. - Advocate for policy and mission level standards used in operational and recurring vulnerability assessments of fielded systems.

Table 3-4. Capabilities and Procedures in CND Protection

a. Information Assurance (IA) is composed of INFOSEC, COMSEC, and COMPUSEC. It is a life cycle process that begins with requirements identification and continues through system design, acquisition, fielding, training, implementation and operation and modification and upgrade. IA capabilities are incorporated into information systems at the beginning of the acquisition cycle and employed throughout the life cycle. USCINCSpace will advocate for mission-level requirements through the preparation and review of Mission Need Statements (MNS), Capstone Requirements Documents (CRD) and Service Operations Requirements Documents (ORD). However, USCINCSpace will not engineer, develop or acquire specific CND capabilities.

b. Education, Training and Awareness. USCINCSpace will advocate for and facilitate CND education, training, exercises and awareness programs. These efforts are essential in providing the background necessary for the development of standards, concepts, technologies, policies, procedures, and operations that enhance the protection of systems and information. (Ref paragraph 3.6.1 .e)

c. Intelligence. USCINCSpace will provide CND indications and warning (I&W) concerning possible threats to information systems by identifying potential adversaries, their intent, and their known and assessed capabilities. USCINCSpace will also support the JTF-CND in leveraging intelligence assets, deconflicting information and disseminating I&W information. In addition, USCINCSpace will correlate, deconflict and, where appropriate, fuse other mission-related intelligence with CND events. (Ref Annex 2, Intelligence Support).

d. Counter Intelligence. USCINCSpace will advocate for policy that strengthens the ability of Counter Intelligence assets to provide I&W of the CND threat. This will include, but not be limited to the establishment of Memorandums of Agreement with LEAs for information sharing, etc. In addition, USCINCSpace will maintain situational awareness of Counter Intelligence efforts in order to deconflict those efforts from other CND initiatives.

e. Risk Management. USCINCSpace will direct action, advocate for policy and support the JTF-CND in determining limits for applying CND countermeasures which affect DoD operations. Risk management includes consideration of information needs, the value of information at risk, system vulnerabilities, threats posed by potential adversaries and natural phenomena, and resources available for protection and defense. Procedures and actions to minimize loss or degradation of information, once discovered, are also an important part of risk management and will be incorporated into the tactics, techniques and procedures of both HQ USSPACECOM and the JTF-CND.

f. Vulnerability Analysis and Assistance. USCINCSpace will coordinate, and deconflict the activities of those organizations and entities that conduct CND vulnerability analyses. USCINCSpace will also act as a "trusted agent" for analysis/assistance activities, when covertly conducted, in order to deconflict them with the current operations and to provide USCINCSpace with CND situational awareness.

g. Vulnerability Assessment. CJCSI 6510.1 B describes four types of vulnerability assessments for system design and operation 1) initial design, 2) testing phase assessment, 3) operational assessment and 4) recurring assessment. USCINCSpace will support this process through advocacy for system capabilities, standards, and policy to support operational readiness and integrity of information systems from system inception to full operational capability,

3.1.2.3. Defensive Operations (Reference Table 3-5). USCINCSpace will advocate for CND policy and operations, and conduct operations that test the viability of CND policy. The objective is to deter threats to INFOSEC or, when deterrence fails, to defeat the threat,

<u>Defensive Operations Activities</u>	<u>USCINCSpace Roles and Responsibilities</u>
Deterrent CND capabilities	<ul style="list-style-type: none"> - Advocate for CND policy and mission level requirements addressing protection capabilities - Conduct CND operations to meet national deterrence objectives
CNA	<ul style="list-style-type: none"> - Lead development, coordination, and execution of offensive COAs to mitigate, defeat, and/or destroy specific threats to DoD networks and systems.
Other Military Operations	<ul style="list-style-type: none"> - Integrate and coordinate CND/CNA COAs with other related military capabilities.

Table 3-5. Defensive Operations in CND Protection

- a. USCINCSpace will develop COAs and advocate for Standing Rules of Engagement (SROEs) for offensive actions in order to support defensive objectives. USCINCSpace will advocate for offensive actions to be integrated with defensive information operations (DIO) to improve response against identified and potential threats to friendly information and information systems,
- b. Selection and employment of specific offensive capabilities will be consistent with U.S. objectives, applicable international conventions, and rules of engagement.

3.1.3. **Detect and assess.** The ability to identify and detect attack/intrusions on computer networks and systems requires close cooperation/coordination with system developers, administrators, users, service providers, civil and military LEAs, and intelligence agencies (Reference Table 3-6.) The process also includes the ability to detect other IO, i.e., deception, psychological operations, etc., against operators of DoD computer networks and systems. The assessment of attack/intrusion encompasses the timely collation of warnings and correlating and characterizing the attack/intrusion activity. Automated methods to **assess** and report system damage and information compromise is essential to effective CND. Detecting, assessing, and reporting are also key for response and restoration after attack/intrusion.

Detection Elements	USCINCSpace Roles and Responsibilities
Computer Network/System Development	- Advocate for computer network/system mission-level capabilities to counter known and anticipated vulnerabilities
Computer Network/System Providers and Administrators	- Provide awareness and education of emergent attack/intrusion techniques and network/system vulnerabilities.
Computer Network/System Users	- Advocate education, training and awareness for recognizing changes and abnormalities in user file content or disturbances in files and awareness of potential threats to and vulnerabilities inherent to media.
Law Enforcement	- Share information of incidents/intrusions with LEA. - Develop procedures to determine conditions and mechanisms for reporting incidents/intrusions to LEAs.
Intelligence and Counter Intelligence	- Provide Indications and Warning. Coordinate between intelligence and LEA, system developers, providers, and administrators.
Reporting Structure	- Provide a continuous functional reporting structure. - Advocate reporting structure for timely collation, correlation, analysis, and warning dissemination. - Keep CINCs and their Component Commanders, JFCs, and JTF Commanders informed of events and impacts to their operations.

Table 3-6. Detection of Attacks and Intrusions

3.1.3.1. The existing JTF-CND processes, and tactics, techniques and procedures (TTP) remain in effect for technically detecting and analyzing attacks or intrusions. Figure 3-2 refers to reporting from bases, camps, posts, or stations to the JTF-CND's service components, as well as GNOSC analysis and interface and coordination with LEA and intelligence agencies. The JTF-CND will receive reports according to existing guidelines, monitor and review CJCS 6510.01 B criteria for technical incidents, and, if necessary, recommend modifications to existing reporting procedures to USCINCSpace. The JTF-CND will continue to manage and publish the alerts, warnings, and notices to the DII community. C/S/A commanders will continue operational reporting of events that affect missions under existing guidance. Examples of these reports are Operations Reports (OPREPs), Situation Reports (SITREPs) INFOCONs, and IAVAs.

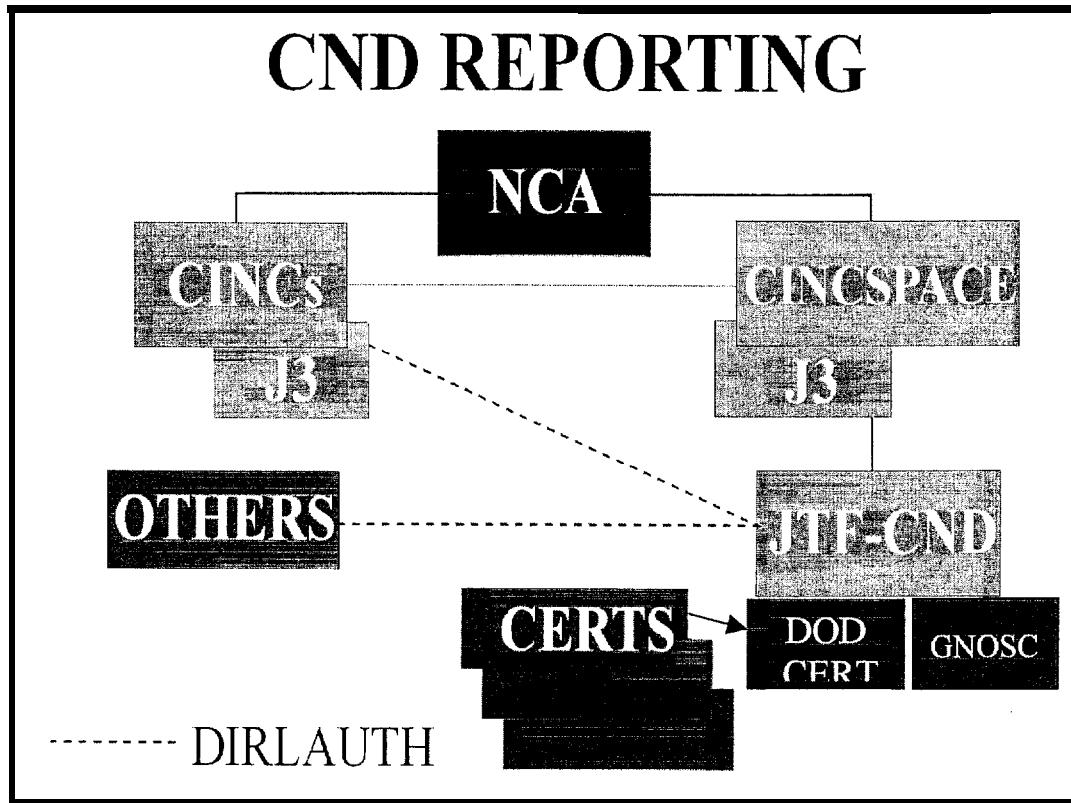


Figure 3-2. CND Reporting

3.1.4. Restore. (Table 3-7) USCINCPAC will advocate for policy and procedures for prioritized restoration of minimum, mission essential, network capabilities. Figure 2-1 describes USCINCPAC's initial priorities for protecting the DII. USCINCPAC will focus on the restoration process tenets outlined in CJCSI 6510.1 B as follows:

3.1.4.1. Advocate for policy and capabilities that provide for decentralized backup/redundant links or system components, backup databases, or alternate means of information transfer.

3.1.4.2. Deconflict deployable restoration assistance capabilities to provide required expertise and tools to restore services. Advocate for capabilities that can provide on-line restoration service.

3.1.4.3. Advocate for automated alert mechanisms that provide enhanced situational awareness and create decision points for system managers and administrators. This capability would provide direction on when to terminate adversary system access. The decision must rely on a risk assessment of continued access, consideration of current and future operations, and intelligence impact.

3.1.4.4. Advocate for policy that provides an inventory system and information resources to identify surreptitious adversary implants after an intrusion/attack has occurred.

3.1.4.5. Implement a reporting system that gathers feedback and lessons learned according to the Joint Universal Lessons Learned System (JULLS) and After Action Report (**AAR**) processes. This information will be included in annual planning documents, standards and procedures for protecting the DII, standing rules of engagement, and restoration plans.

3.1.4.6. C/S/As must evaluate their restoration procedures and balance them against operational mission requirements and the overall effect on the DII.

Restoration Elements	USSPACECOM will:	1
Backup/Redundant Links	Advocate for decentralized alternative means of info transfer	
Inventory tools and techniques	Advocate for capabilities techniques and procedures that provide for inventory of systems after intrusion has occurred to detect intruder implants	
Automated decision support	Advocate for automated decision support tools that provide system managers ability to know what basic action to take with regard to CNAs	
On line or deployable Restoration assistance	Coordinate and deconflict deployable resources. Advocate for on line restoration capabilities	
Post-attack analysis	Provide after action information on attack/intrusion lessons learned	

Table 3-7. Restoration after Attack or Intrusion

3.15. Respond. (Table 3-8) The attack/intrusion response process involves determining actors and their intent, establishing cause and complicity, and possibly taking appropriate actions against perpetrators. Response is an integrated, coordinated, and focused defensive effort to cope with, reduce, or eliminate the effects of attacks or intrusions on the DII. The process contributes to information environment protection by removing threats and enhancing deterrence. Actions directed by USCINCSpace may include:

3.1.5.1. Change of DoD-wide INFOCON, system passwords, or in extreme conditions, system shut down. (Ref figure 2-3).

3.1.5.2. Recommend, to the NCA (in coordination with theater CINCs) diplomatic action and/or economic sanctions against a hostile foreign nation.

3.1.5.3. Recommend, to the NCA the use of military force.

3.1.5.4. Establish effective mechanisms to assess, coordinate, and report, to include teleconferences, messages, SIPRNET/GCCS postings, and other secure methods (Ref

paragraph,' 3.3 CINC Assessment Process). The focus of reports will be on effective and timely actions to protect the DII. USSPACECOM will also advocate SROEs, unified instructions, and TTP to respond to attacks or intrusions against the DII.

3.1.5.5. As appropriate, approved models from the Joint Operational Planning and Execution System (JOPES) and the Crisis Action Planning process will be used to develop, plan, and carry out responses to attacks and intrusions. For activities isolated to the DII networks, USCINCSpace will submit a CINC's assessment message to the JCS, according to current guidelines and practices. Depending on the situation, this message may cause the JCS to respond via a planning order and identify the supported and supporting CINCs.

3.1.5.6. Pre-planned responses may include adding personnel, deploying response teams, and procedures. USCINCSpace will task the Commander, JTF-CND and others for response options, then coordinate these options with national agencies or others and assemble them into courses of action. Responses may be cyber and/or physical. For situations that involve attacks/intrusions beyond electronic attacks on the DII, USCINCSpace will recommend to the NCA the cyber and space responses and help integrate them with the supported CINC's overall campaign. Continued review and feedback on the response process will funnel lessons learned back to standards, policies, and procedures for CND.

3.1.5.7. USCINCSpace delegates specific authority to the Commander, JTF-CND to direct selected CND actions in defense of the DII. The JTF-CND Commander will develop and forward to USCINCSpace, if required, courses of action and assessments. However, most CND actions will fall within the purview of the JTF-CND's scope of authority and won't require a CINC assessment. JTF-CND will characterize, assess, and act on attacks and intrusions according to the delegated authority. When appropriate, USCINCSpace will provide a CINC's assessment message to the CJCS providing recommended COAs regarding a potential hostile force and request support to eliminate the threat. This will be done in accordance with standard JOPES processes. The key is identifying the attacker. This will require a coordinated effort with LEAs, Counter Intelligence (CI), the Intelligence Community, and many others. Both DoD and DoJ have concurrent jurisdiction during all phases of an incident.

Response Elements	USSPACECOM will:
Law Enforcement	Support and deconflict LEA CND efforts
Economic Sanctions	Recommend to NCA in coordination w/Theater CINCs appropriate economic sanctions to deter/curtail CNA activities
Military Force	Recommend to NCA in coordination w/Theater CINCs appropriate military Force
Diplomatic Actions	Affect Diplomatic Actions through Theater CINCS to deter foreign CNA activities

Table 3-8. Response to Attacks and Intrusions

3.2. USSPACECOM CND Operational Relationships. (Ref Figure 3-3). HQ USSPACECOM will focus on policy, process, mission-coordination, integration and direction, while the JTF-CND will focus on operational mission execution. HQ USSPACECOM will interact with the C/SAs (CINCs, Services, JS, OSD, DoD agencies, DISA, IC, NSA, LEAs, NIPC, industry, etc.) to integrate support and continuously improve the DoD's CND process. These process-oriented activities will complement the JTF-CND's mission execution responsibilities.

USSPACECOM CND RELATIONSHIPS

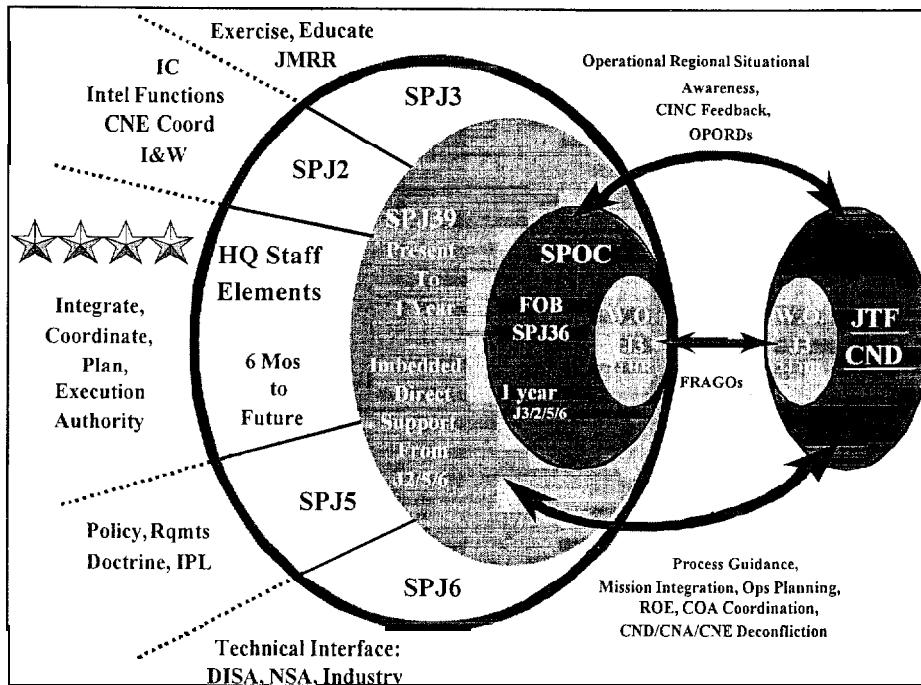


Figure 3-3 USSPACECOM CND Relationships

3.2.1. USSPACECOM

3.2.1.1. The USSPACECOM (SP)/J36 Space Operations Center (SPOC) provides a continuous (24 x 7) capability and has developed interactive relationships with other CINC's operations centers. Their daily interactions will provide enhanced situational awareness of current military operations and exercises. USCINCSpace will provide enhanced situational awareness of on-going military operations to the JTF-CND (through a CND watch officer in the SPOC). The watch will evaluate the impact of the CND event and the JTF-CND directed actions on real world operations. Updates and interim guidance to the JTF-CND will be issued by CINCSpace via the CND watch officer through fragmentary orders (FRAGO).

3.2.1.2. The J36 SPOC Future Operations Branch (FOB) will focus on operations and planning, 24 hours to 1 year in the future. The FOB interacts frequently with other C/SAs to map out planned space support requirements. For the CND mission, a matrixed support team of J2, J3, J5, and J6 personnel will provide direct CINC-level

support to the JTF-CND. The J36 FOB will provide USCINCSpace guidance to the JTF-CND via bi-monthly operations orders (OPORD). This guidance will include insights into any known or planned military operations, exercises, or other situations that could be affected by JTF-CND directed actions. This is a similar process that other CINC's use to direct their components or JTFs.

3.2.1.3. The SP/J39 is a matrixed organization that integrates and leverages J2, J3, J5 and J6 expertise. SP/J39's time horizon is from current operations out to 1 or 2 years. J39 coordinates and integrates USSPACECOM support to C/S/A and allied operations for the DOD CND mission. SP/J39 will develop and coordinate process oriented guidance for the CND mission in the form of unified instructions, concepts of operations, ROE, and other documentation as required. SP/J39 will develop and coordinate CND-specific support plans for other CINCs' OPLANS and CONPLANS. These support plans will be more inter-theater focused and will complement the regional plans developed by the other CINCs. In addition, SP/J39 will coordinate mission support and integrate the efforts of C/S/As to provide an operational focus to the overall DOD CND mission. For crisis support, SP/J39 may augment the JTF-CND or the SPOC. Finally, SP/J39 matrixed personnel will interact frequently with its parent J-staff directorates to ensure consistency of support to the DOD CND mission. These personnel will provide the conduit to their parent directorates for operational insights into the CND mission. They will draw upon those directorates for additional support when needed. These matrixed personnel will physically reside within J39 and will be dedicated to the CND mission.

3.2.1.4. The preceding paragraphs describe HQ USSPACECOM divisions directly engaged in support of CND mission execution. Additionally, headquarters staff elements not directly engaged in mission execution, nonetheless still provide important, long-term CND mission support. The following section briefly highlights general functions for each directorate:

3.2.1.5. SP/J2 will coordinate with the intelligence community to identify, manage, monitor, and advocate for CND intelligence requirements, standardized reporting, enhanced collection management, etc. The SP/J2 will also derive indicators from deliberate planning activities to focus monitoring, collection, and analysis activities, with the goal of providing enhanced I&W and value-added analysis for DoD CND efforts.

3.2.1.6. SP/J3 will organize, advocate, and coordinate CND exercises across C/S/As. The SP/J3 will advocate for standardized training and education requirements, and coordinate CND modeling and simulation efforts. In addition, SP/J3 will produce a Joint Monthly Readiness Review for the DoD CND mission and force structure. This will be based in large measure on inputs from the JTF-CND, but also on frequent interaction with C/S/As.

3.2.1.7. SP/J5 will develop, coordinate and advocate for CND, concepts, policy, doctrine, Integrated Priority List, and mission-level requirements. In addition, SP/J5 will assist in development and support of command and DoD partnerships with selected industry, academia and allies, including development of the necessary memoranda of

agreement/understanding (MOA/MOU). They will develop a Colorado Springs Technology Center of Excellence for training and education, career development and professional growth.

3.2.1.8. SP/J6 will serve as the technical CND subject matter experts on the USCINSPACE staff. The SP/J6 will support development of partnerships and relationships with DoD and non-DoD agencies, private industry, and coalition partners. In addition, SP/J6 will help develop and advocate for common education, training, and awareness standards for users, operators, and administrators. Finally, SP/J6 will help ensure CND requirements are reflected in plans, requirements, and courses of action.

3.2.1.9. USCINCSpace staff actions will complement and support other C/S/As, not usurp their responsibilities. No other CINC, Service or agency is currently performing these tasks to provide this level of integrated and responsive CND mission support, worldwide.

3.2.2. JTF-CND

3.2.2.1. The JTF-CND executes the CND mission. Its focus is procedural and operational, requiring close coordination with the C/S/A's for information sharing necessary in the analysis and assessment process. The JTF-CND provides inputs to HQ USSPACECOM for policy, planning, ROE, requirements, and mission processes. However, its primary responsibility is to carry out the daily execution of the DoD CND mission. JTF-CND's time horizon is focused on current operations.

3.3. Commander's Critical Items of Information. JTF-CND reporting criteria to USSPACECOM will be based on whether a situation requires immediate attention, or can be reported via routine channels. Immediate Situation Reports are required when a situation is reported that falls within Category 1 or Category 2 criteria. However, the CJTF-CND may contact USCINCSpace directly, when it is determined that a situation requires a time critical discussion or direction. The three mission categories are identified below, with corresponding criteria.

3.3.1. Mission Category 1. This category requires USCINCSpace involvement. The JTF-CND WO will immediately notify the USSPACECOM SPOC when a situation meets Category 1 criteria.

3.3.1.1. Criteria 1 Examples:

- a. The CJTF CND determines a change to the DOD INFOCON level is warranted.
- b. The CJTF CND needs to direct actions that negatively affect C/S/As' operations.
- c. The CJTF CND recommends that USCINCSpace notify the NCA of the situation.
- d. CJTF CND directed actions that could negatively impact real world operations.

3.3.2. Mission Category 2. Time sensitive notification. Category 2 criteria requires notification to the USSPACECOM senior leadership (e.g. J3, DCINC, CINC), but does not require a USCINCSpace decision. When a situation meets Category 2 criteria, the JTF CND WO will notify the USSPACECOM SPOC as soon as is practical.

3.3.2.1. Criteria 2 Examples:

- a. An INTRUSION or INCIDENT into any DoD closed network or the SIPRNET.
- b. Unauthorized privileged user, administrator or root level access of a DoD computer system.
- c. An INTRUSION or INCIDENT into the NIPRNET when the nature of the activity is such that it will likely gain adverse civilian media and/or general public attention. For example, the modification or defacement of a high government level Web Page (such as OSD) that receives frequent public access.
- d. An INTRUSION or INCIDENT that reports the denial, disruption, degradation, or destruction of information or information networks, and is assessed (by the operator) as impacting military operations. Examples include impacts to information that supports:
 1. Employment/deployment of U.S. forces
 2. Intelligence support to military systems
 3. DoD logistics
 4. DoD communications systems
 5. DoD space, air; land, and sea systems
 6. DoD personnel, medical, or finance systems
- e. An INTRUSION or INCIDENT regarding the deception or theft of information and/or information systems directly affecting National Security. Examples include:
 1. Mission critical information related to Weapons of Mass Destruction or Chemical/Biological weapons
 2. Potential terrorist activities
 3. Potential state-sponsored espionage activities

3.3.3. Mission Category 3. Routine operations. Category 3 criteria are routine situations that do not require special notification to the USSPACECOM SPOC. Instead of direct reporting, the JTF CND WO will include Category 3 events on the CND Operations Report-t. Mission Category 3 situations require JTF CND action, but do not meet the Category 1 or 2 criteria listed above.

3.3.3.1. Criteria 3 Examples:

- a. Do not require USSPACECOM staff involvement/assistance.
- b. Do not negatively impact real world military operations.

leads to ambiguity

c. Involves the theft/deception of information or information networks and is assessed (by the operator) as no immediate impact to military operations.

d. Requires the notification and involvement of military or civilian law enforcement resources.

Define

3.3.4. Routine Reporting. Routine activity includes incidents that constitute an intrusion and/or ~~attack and the response~~ actions that may require USSPACECOM staff action but do not require USCINCSpace assessment or direction. JTF-CND reporting to the SPOC provides USCINCSpace with CND situational awareness and informs the HQ USSPACECOM Staff of events and issues that require their attention and assistance. Reporting is accomplished through voice, AUTODIN messages, GCCS text messages, SIPRNET email messages, or Odyssey Collaboration System (OCS) messages.

3.3.4.1. Operations Report. The baseline report of CND operational activity is the *Op Rep* Operations Report. This report, prepared by the JTF-CND, is designed to provide a summary of CND activity to the USSPACECOM/J3 twice weekly, on Tuesday and Friday of each week. Suspense time for delivery to the USSPACECOMN3 and other addressees will be stated in the governing mission order. Information copies will be provided to the other C/S/As, unless otherwise directed, for the purpose of situational awareness. The following paragraphs list the type of information reported in the Operations Report:

a. INFOCON Summary Report *changes, by exception*, on the status of all C/S/As' INFOCON postures and the overall posture of the DII. Include explanatory comments for levels and changes.

b. Operations Tempo. Report the metrics and/or statistics that communicate an accurate picture of the level of CND activity experienced over a given period of time. This information provides background data for use in resource justifications, reference material for priority and tasking direction, etc. Suggested content includes, but is not limited to, summary and total of activities engaged that require CND Watch Officer (WO) actions, number of these activities which resulted in incidents and/or intrusions, number of incidents/intrusions opened and/or closed, etc.

c. Significant Activities. Provides the total number of significant activities the JTF CND is tracking ("significant" activities are defined as computer network activities that meet USSPACECOM Mission Category 1, 2, or 3 criteria). For each activity, the report provides:

1. JTF CND File Number
2. USSPACECOM Mission Category (1, 2, or 3)
3. Location of C/S/A reporting the activity
4. System affected (SIPRNET, NIPRNET, or Other)
5. Reporting C/S/A

6. Description of activity, to include (as available) the appropriate CND Taxonomy term, a textual description of the problem, a description of the unauthorized result, identity of the intruder, and any other information relevant to the situation
 7. Operational impact to reporting center's mission operations - *who's Assess now?*
 8. CJTF assessment of significance
 9. JTF CND directed actions (beyond any already directed by the reporting C/S/A)
 10. Status update from last report
- d. Upcoming exercises and dates
- e. Additional JTF CND comments as required.

SITREP

JTF + C/N

3.3.5. **Non-Routine Reporting.** The **Situation Report** will be used by the JTF-CND as a means to report mission category 1 and 2 events to USCINCSpace via USSPACECOM/J36S. The Situation Report does not preclude communication by other means, when time is critical. However, in such time critical instances, a formal Situation Report will prepared as a follow up.

3.3.6. **Data Gathering.** During analysis and evaluation of incidents, the JTF-CND will conduct data gathering inquiries-11 associated C/S/As, to include USSPACECOM. The purpose is to identify and correlate the scope of the incident and impact to network operations across the DII. The JTF-CND will provide the C/S/As the known information related to the incident such as affected locations, immediate impact, potential effects, etc. The primary USSPACECOM point of contact for the JTF-CND is the SPOC WOMNCO. The SPOC Watch Officer/Watch Noncommissioned Officer (WOMNCO) is responsible for identifying, correlating, and providing the JTF-CND with the incident's impact to USCINCSpace's space operations. This includes coordination, **as** required, with the HQ staff and USSPACECOM space components. The duration and extent of the data gathering process varies greatly due to the nature of computer security incidents. The primary means of communication between the JTF-CND and the C/S/As is message traffic, SIPRNET, and voice communications. These messages/conversations may be individual or collective and are informal in the sense that they are not a missile/space warning type voice conference with mandatory attendees, role call, etc. Research into the ability to migrate this process onto a computer based collaborative system, i.e., GCCS or SIPRNET based OCS Tool, will be evaluated as the procedures mature.

3.3.7. **Response COA Development.** The JTF-CND, and its supporting components, will develop the appropriate technical and operational response actions required to counter or mitigate attacks and intrusions into the DII, to include actions required for restoring the DII. The COAs are technical in that they involve the network management and administration details of the DII networks. The COAs are operational in that they are integrated and coordinated with mission priorities, timing, and objectives that may not always match the most expedient or effective technical restoration actions and timelines. These COAs are based on available plans, SROE, information provided by

the C/S/As, and crisis planning/coordination by the JTF-CND staff, to include the GNOSC and DoD CERT. These COAs may be as simple as directing no further actions than previously directed by the JTF-CND's service components, or as complex as integrated, timed actions executed across the DII. For discussion on the intelligence support to COA development, reference paragraph 4.1 of this CONOPS, and Annex 2.

3.3.8. Authority Determination. In accordance with the delegated authority from USCINCSpace, the CJTF-CND will act autonomously to direct and execute the CND mission. The CJTF authority is bounded by thresholds of activities, noted in paragraph 3.3.3.1, that require USCINCSpace assessment and direction. The CJTF-CND has discretion, based on USCINCSpace guidance, over determining whether the JTF-CND's response actions require USCINCSpace involvement. The CJTF has autonomous authority to act on behalf of USCINCSpace except in the following cases:

3.3.8.1. When directed response actions will negatively impact the ability or effectiveness of supported CINCs to accomplish their assigned missions. This includes ongoing or pending real world contingency or crisis operations. Impact to operations refers to mission/operations degradation or failure. Impact does not refer to convenience or common practices that do not impede the mission. Care must be taken to determine whether the disruption of common convenience practices will create such confusion as to actually impede or disrupt mission operations. Examples:

- a. Affect command and control of a CINC's, joint force commander's, or JTF's force structure.
- b. Stop or disrupt an ongoing campaign.
- c. Create impassable barriers to the interconnectivity between computer-based equipment/systems.
- d. Direct actions that divert a CINC's resources from accomplishing the planning and execution of an upcoming operation.

3.3.8.2. When directed actions require a change to the DoD INFOCON posture. *DOD US. CINC INFOCON?* CINCs, local commands, and agencies may increase their INFOCON for forces under their control, but an across the board DoD INFOCON change has potential ramifications in the areas of national policy and strategic indications and requires USCINCSpace coordination.

3.3.8.3. When actions require notification or interaction with the CJCS or NCA. Like DoD INFOCONs, these are actions with significant national policy and security implications and require USCINCSpace involvement. Examples:

- a. Announcement of a significant vulnerability within the DoD or to national security that may be exploited by foreign government or computer intruders.
- b. Implementation of capabilities determined to require NCA coordination and approval.

3.3.9. Execution. The JTF-CND will continue to be the conduit for dissemination of CND mission direction. The CJTF-CND executes the CND mission operations under USCINCSpace's delegated authority. This includes dissemination of the direction for the selected COAs, coordination of timing or other implementation requirements, monitoring of the execution and attainment status, modification of COAs as required, and reporting of after actions and lessons learned.

3.3.10. USSPACECOM Staff Actions for Routine Activities and Reportins.

3.3.10.1. General Support Activities. The JTF-CND executes the CND mission. HQ USSPACECOM supports the JTF-CND's activities both directly and indirectly. The following are anticipated actions taken by the USSPACECOM staff that do not require assessment and direction of USCINCSpace.

a. Situation Monitoring. HQ USSPACECOM will monitor the ongoing situation and status of forces. The SPOC WO/WNCO will maintain situational awareness and connectivity with the JTF-CND through the message traffic and Operations Report. This information flow is a push action from the JTF-CND except where additional information or clarification is required from the HQ staff. Automation and the use of web tools are encouraged as the process matures. Watch officers and command staffs will communicate across organizational boundaries with their counterparts. This will alleviate the watch from managing information not directly related to the ongoing current operation.

b. CND Operations Reports. Reports from the JTF-CND are received and monitored by the CWO/NCO. The reports are passed to J36S, SPOC, and J36P, (FOB); information addressees are J39C, the CND/A Branch; J2F, Combined Intelligence Center, and J6O, Operations Branch for situational awareness and monitoring of problems or issues requiring HQ staff actions. This provides the J6 timely awareness of CND-related problems/issues and allows J6 to expedite internal responsibilities for technical support to USCINCSpace space operations and technical support to CINC NORAD ITW/AA operations. The CWO/NCO uses the reports to brief the USSPACECOM senior leadership through special situation briefs or the routine operations/intelligence briefs. The CWO/NCO and/or the FOB, depending on the timeframe of required actions, will use the reports to update or modify the standing mission orders for the CND mission. Both are supported by J39.

c. Data Gathering. USCINCSpace responds to JTF-CND data inquiries in the same manner as all C/S/As, by evaluating the situation and incidents identified by the JTF-CND against assigned missions. USSPACECOM correlates the JTF-CND information with space events or space related activities and evaluates the impacts on current and future space operations. The CWO/NCO is responsible for interfacing with the Headquarters USSPACECOM, CMOC (Cheyenne Mountain Operations Center), and space components to determine correlation and impacts. The CWO/NCO's primary means of communications with CMOC and the space components are by message and secure voice. This information is passed back to the JTF-CND for situational awareness and identification of the scope of the incident. The information is also used

to update the USSPACECOM staff and leadership during special situation briefs or the routine operations/intelligence briefs.

3.3.10.2. Impact on Space Operations. If a CND incident is correlated to a space event or space-related activity, the CWO/NCO will integrate CND operations with the SPOC WO and space operations. Existing procedures are used to evaluate, characterize and report space-related incidents to the appropriate parties. The CWO/NCO will continue to keep the JTF-CND informed of progress and actions associated with space operations for the purpose of JTF-CND situational awareness and coordination with CND response activities.

3.3.10.3. Implementing CJTF actions. The CJTF will direct the development and execution of COAs in response to specified CND incidents. USSPACECOM will implement the directed actions on the networks under its control in the same manner as all C/S/As. N/SP/J60 will lead the internal USSPACECOM implementation actions and report successful implementation back to the CWO/NCO or FOB. Internal USSPACECOM response actions to a CND incident, as with all C/S/As, must be integrated with the CJTF directed actions. Upon completion of the directed actions, the CWO/NCO will report attainment to the JTF-CND. The primary means of communication are the same as mentioned in paragraph 3.2.7.1, a and c above. If USSPACECOM cannot implement the response actions in accordance with the CJTF directed methods, timing, or procedures the CWO/NCO must inform and coordinate non-compliance with the JTF-CND.

3.3.10.4. Headquarters Staff Support to CJTF. The HQ USSPACECOM staff supports the JTF-CND in executing CND operations. Support requirements will be coordinated and prioritized based on the need and available resources. Requirements may be communicated through the Watch, between staff elements, or through the CJTF's DOR, depending on their relevance and importance. Examples of such activities are policy research and advice, resource requests, coordination or intervention with another C/S/A's staff, exercise coordination, etc.

3.4. USCINCSpace Assessment Process. (Ref figure 3-4). This paragraph describes the level of activity and operations that require response actions exceeding the thresholds of CJTF's delegated authority and require USCINCSpace assessment and direction. Methodologies for operations internal to the JTF-CND will be described in detail in the JTF-CND CONOPS and TTPs.

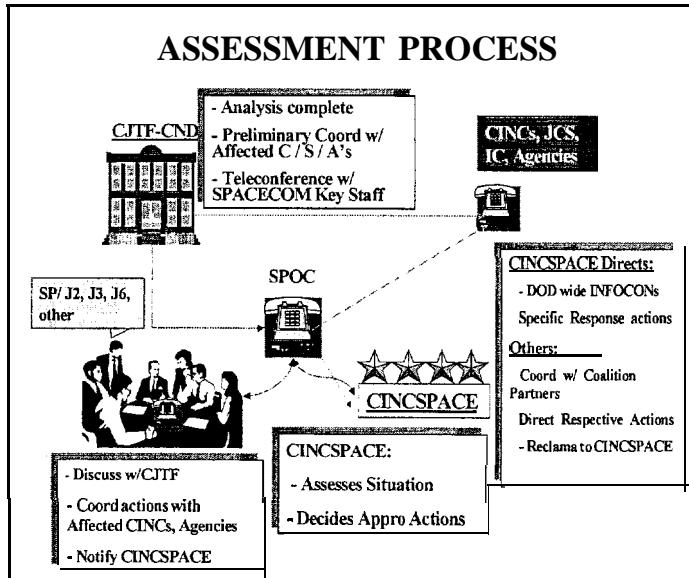


Figure 3-4 CINC Assessment Process

3.4.1. Authority Determination. The same actions described in Routine Activities and Reporting, above, are taken up to the point of disseminating the CJTF-directed actions or response to CND incidents. At the point where CJTF determines that directed actions will breach an established threshold, the CJTF must obtain assessment and direction from USCINCSpace prior to implementing such actions. The CJTF must determine what portion or aspects of the overall response will breach the thresholds and which portions or aspects can be implemented autonomously. Timing, integration, and coordination may allow piecemeal implementation of non-breaching actions or necessitate USCINCSpace assessment/direction prior to any implementation.

3.4.2. The CJTF has the responsibility and authority to communicate directly with USCINCSpace, without USSPACECOM staff interface, should timeliness or criticality of a CND incident dictate. However, when required action is not time dominant, the HQ USSPACECOM staff and the CJTF will discuss, coordinate, and refine (if required) the COAs which involve threshold breaching actions. The JTF-CND will contact the CWO/NCO to initiate a CND threat conference (via teleconference or video teleconference) with the CJTF and the USSPACECOM J2, J3, and J6. These meetings may be a single gathering or several meetings, as the situation requires. Depending on the situation, the USSPACECOM J3 may direct the forming of a Crisis Response Cell (CRC), Crisis Action Team, or recall of the Battle Staff. When agreement is reached on the COAs, the CJTF presents them to the USCINCSpace for assessment and direction. If required, the HQ staff will present relevant space related issues affected by or affecting the CND COAs. As with coordination conferences between the CJTF-CND and USSPACECOM principal staff officers, USCINCSpace's assessment may continue over multiple briefings and discussions.

3.4.3. Execution. The JTF-CND will serve as the conduit to the C/S/A for the execution of USCINCSpace direction. On behalf of USCINCSpace, the J3 will provide guidance to the CWO/NCO, FOB, or Crisis Response Cell (CRC) for inclusion or update

into the appropriate mission orders. If required, the CJTF can execute on the verbal direction of the CINC. However, the SPOC, FOB, or CRC will provide the JTF-CND with revised orders as soon as possible.

3.4.4. USSPACECOM Staff Actions in Support of CINC Assessment Process

3.4.4.1. The primary focus of the HQ staff is to validate the impact of the CJTF's recommended COAs on DoD operations, National and DoD policy, CJCS and USCINCSpace guidance and correlate them with space support issues in order to facilitate the CINC's assessment and direction.

3.4.4.2. Conferences. The SPOC CWO/NCO is the primary OPR for facilitating the JTF-CND's requested teleconferences/VTCs with USSPACECOM's principal staff officers. The CWO/NCO will notify the USSPACECOM principal staff officers of the situation and will initiate required actions for establishing the teleconference/VTC.

3.4.4.3. CINC Direction. The J3 will provide the CINC's direction to the CWO/NCO for inclusion into or update to the mission orders to the JTF CND. Normal procedures for update to these orders will be used.

3.4.4.4. CINC Reports. The JTF CND disseminates the required operational information and direction resulting from the CINC's assessment. The CWO/NCO, in coordination with the HQ staff, will develop and disseminate CINC level reports required to inform the CJCS, SecDef, etc. Examples of such reports may be a CINC assessment message that initiates the JOPES process, requests for support or Personal For (P4) messages.

3.5. Deliberate Planning. USCINCSpace, through the J3, coordinates the USSPACECOM staff in implementing the tasking and guidance contained in the Joint Strategic Capabilities Plan (JSCP) by publishing an OPLAN or CONPLAN and supporting plans, as required. CND operational planning will follow the standard Joint Planning Process (JOPES Vols I, II, III).

3.5.1. The objective of USSPACECOM deliberate planning is to provide a framework, similar to OPLAN 3500-99 (Space Operations in Support of Regional Contingencies) that supports CINCs in the development of CND annexes to their specific OPLANS, and enhances indication and warning capabilities for effective CND.

3.5.2. USSPACECOM deliberate planning will focus on inter-theater protection of the DII in order to support the execution of supported CINCs' OPLANS. USSPACECOM OPLANS/CONPLANS and supporting plans will describe potential avenues and methods of attack/intrusion an adversary could use against the DII. It is particularly important to provide an understanding of CND interdependencies among the CINCs, Services, and Agencies, because computer network attacks/intrusions in one area, and actions taken to defend against them, can create vulnerabilities in another area. Examples USCINCSpace inter-theater support are as follows:

A US and AF

3.5.2.1. TPFDD execution.

3.5.2.2. Functions/activities/ops outside the supported CINCs AOR

3.5.2.3. Ensure CND actions across DoD are performed to support execution of OPLAN.

3.5.2.4. Identify potential indicators.

3.5.2.5. Derive Priority Intelligence Requirements (PIRs).

3.5.2.6. Focus monitoring activities.

3.5.2.7. Events that could affect OPLAN or contingency plan execution.

3.5.3. USSPACECOM, in conjunction with the JTF-CND, will develop courses of action for CND that fall into three Dies. CND
passive, active & offensive

3.5.3.1. Passive defense COAs will be developed to protect and defend the DII, which include such measures as configuration control of the networks, password changes encryption, and INFOCON changes. Each of these defensive actions must be weighed and mitigated to assess risk and impact throughout the DII before implementation.

3.5.3.2. Active defense COAs are those that may require interaction with law enforcement/CI agencies to effect warrants for arrest, court orders, or other response actions. Other areas for planning in this category may entail counterintelligence and/or diplomatic initiatives.

3.5.3.3. Offensive actions are those COAs that plan for computer network attack (CNA) against adversaries and seek to preclude impending attacks. They include trace back, hack back, beaconing, -and physical attack. When physical attack is recommended, COAs will be submitted to the Chairman, Joint Chiefs of Staff (CJCS) for approval, where upon a supported CINC will be designated for COA execution.

3.5.4. USCINCSpace will assist other CINCs in the development of their IO/CND OPLAN annexes by providing supporting documentation and technical support on the current CND environment, including OPLANS, CONPLANS and supporting plans. USSPACECOM/J39 has responsibility for the coordination of IO/CND planning support. This support may be as simple as exchanging documentation or as complex as coordinating the deployment of an assistance team. Requests for planning support will be made through the USSPACECOM SPOC to J39.

OK
3.6. Crisis Action Planning. The USSPACECOM J3, through the SPOC, will oversee the execution of the CND CONPLAN or OPLAN in time of crisis or during exercises. The SPOC will effect the plan execution by issuing mission type orders to the JTF-CND and USSPACECOM components. Changes to the CONPLAN/OPLAN will be made

through the issuance of fragmentary orders (Frag Orders). When the operations tempo exceeds the SPOC's ability to manage it, J36 may recommend the Crisis Response Cell (CRC) be formed. If the crisis demands 24/7 support, the J36 will recommend to the J3 to form the Crisis Action Team (CAT). If the crisis requires the participation and 24/7 attention of the directorates and the CINC, the J3 may recommend to USCINCSpace that the Battle Staff be recalled.

3.7. Support Requests. The USSPACECOM HQ Staff will be responsible for responding to and coordinating a variety of support requests from the C/S/As. CINCs will utilize assigned Space Liaison Officers (LNO) to coordinate support requirements. Services and Agencies not assigned LNOs will forward requests for support to the SPOC for coordination and resolution. Requests may be made via phone or via GCCS on the SPOC's homepage. If the request is outside the SPOC's scope of responsibilities, the SPOC Watch Officer will ensure the request is promptly forwarded to the USSPACECOM J39 for staffing and resolution.

3.7.1. Requests for support may cover a wide variety of mission areas. The following paragraphs provide examples of support requests that USSPACECOM staff elements may expect to receive:

3.7.1.1. Support to the deliberate planning process as described above.

3.7.1.2. Clarify CND standards and policies. As new and more detailed standards and policies are developed and approved, USSPACECOM must be able to assist C/S/As in the promulgation, interpretation and implementation of these standards and policies. In addition, the USSPACECOM staff will resolve instances where a C/S/A requests relief from a prescribed standard or policy. If required, the staff will assess the potential technical and operational impacts if a stated standard or policy is not fully implemented, then recommend a course of action to USCINCSpace.

3.7.1.3. Intelligence data support. When required, USSPACECOMN2 must be prepared to support, represent, and clarify C/S/A intelligence requirements to the Intelligence Community (IC).

3.7.1.4. Technical Assistance. USSPACECOM must be prepared to respond to technical queries from C/S/As as they implement new CND technologies. While it is not expected that the staff will necessarily be able to address all issues, they must be able to identify and coordinate whatever appropriate technical resources are required to address the specific technical issue(s). Resources may include USSPACECOM/J6 technical support staff, or personnel from the JTF-CND, GNOSC, or other supporting agencies.

3.7.1.5. Training and Certification Activities. (Ref Figure 3-8). As the Command's focal point for CND education, training, and awareness, USSPACECOM/J37 will assist C/S/As in establishing standards and requirements for users, operators, and CND professionals. Specific examples of support could include providing technical resources to assist in course/certification development activities, advocating specific education

and training requirements to technical and mission-level courses and training institutions, and partnering with industry and academia to incorporate innovative concepts.

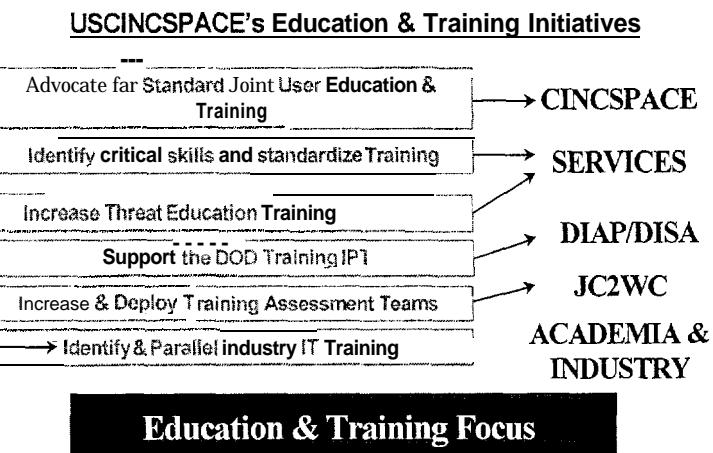


Figure 3-5. USCINCSpace Training and Education Initiatives

3.7.1.7. Staff Assistance Visits (SAVs). When requested, USSPACECOM will coordinate SAVs to assess the implementation, effectiveness, and operational readiness of the requesting C/S/A's CND programs. Resources for conducting SAVs will be integrated from within the USSPACECOM staff and other supporting service and agency elements.

3.7.1.8. Exercise Planning and Participation. USSPACECOM/J37 will advocate for, develop, coordinate, sponsor and support joint and multi-command exercises. In addition to exercise planning, exercise participation will further training and proficiency objectives supporting the integration and application of CND within a C/S/A's Area of Responsibility (AOR).

3.7.1.9. Legal Policy Issues for CND. USSPACECOMNA will work closely with the USSPACECOM Staff in order to anticipate and resolve legal issues that might arise during CND operations. The existing legal framework was not developed with the current technological/threat environment in mind. Along with the J2/3/5/6/POLAD, JA will work the appropriate domestic and international entities to develop a legal and policy framework that permits USSPACECOM and the C/S/As to conduct successful CND operations.

3.7.1.10. Analyzing and Assessing Vulnerabilities. Similar to requests for Red Team or SAV support, the C/S/As may request less formal assistance in analyzing and assessing vulnerabilities. This analysis may include in-depth vulnerability analysis of specific segments of the DII residing within the C/S/A's domain. It may also include a request for assessment of specific or general threats against a computer network or support to policies and procedures regarding CND. There are many organizations analyzing and assessing vulnerabilities of systems. USSPACECOM will maintain a

situational awareness of major assessments ongoing in the DoD. Major organizations (several organizations listed also have multiple internal organizations performing this function) performing this function include, but are not limited to: NSA, DISA, Service CERTs, MAJCOMs, IG staffs, and auditors. Due to potential conflict with real world CND activities, USSPACECOM must be aware of major assessments. Specific consideration will be given to components and organizations under USSPACECOM TACON (i.e., service components and GNOSC/DoD-CERT).

3.7.2. The various requests outlined above provide examples of some non-crisis scenarios and resources that USSPACECOM must be able to provide to its various C/S/A customers. In order to maximize CND support to the C/S/As, the USSPACECOM staff must possess a general knowledge base and, in some cases, a specialized skill set in order to provide the required resource support. Some of the knowledge areas required for USSPACECOM staff involved in CND support include development and understanding of the following:

3.7.2.1. USSPACECOM capabilities to support C/S/As in their planning, training, and exercise activities.

3.7.2.2. Processes, Policies, and Doctrine (PP&D) for CND.

3.7.2.3. Tactics, Techniques, and Procedures (TT&P) for CND during peacetime and crisis.

3.7.2.4. The resources available for expertise, service, and tools beyond the current scope of C/S/A resources and capabilities.

3.7.2.5. What technical support national agencies and other supporting organizations can provide and how to coordinate it to support the C/S/A's CND mission.

3.7.2.6. The C/S/A's needs for possible change in PP&D and their need for improved CND capabilities. The staff must be able to "pull" this information back to USCINCSpace for appropriate changes or advocacy in the CINC's Integrated Priority List (IPL).

3.8. Red Team Resources and Support. USSPACECOM will deconflict computer network Red Team support to assist in exercise or stand-alone training activities. The requirement to deconflict this support, while not currently staffed through the C/S/As, is important to enable immediate discrimination between exercise activity and actual intrusions. It will also alleviate unnecessary stress on network monitoring during time of contingency and crisis. Requests for Red Team support will be received by the SPOC and forwarded to USSPACECOM/J39 for action.

3.9. Exercises. USCINCSpace will sponsor and support a yearly level 1 CND exercise to maintain readiness and increase proficiency. USSPACECOM will conduct exercises focused on CND support to other CINC's. Additionally, as a supporting CINC, USCINCSpace will advocate incorporating CND into all other exercises and wargames and selectively coordinate exercise support to regional CINC's. Based on exercise

APOLLO CND PLANNING	Date from Execution (E) Day
Concept Development Conference	E-270 days
SPJ3 Proposed Commander's Intent Brief	E-210 days
UD Proposed Commander's Intent Brief	E-200 days
USCINCSpace Commander's Intent Brief	E-195 days
USSPACECOM Initial Planning Conference	E-180 days
USSPACECOM Mid Planning Conference	E-I 35 days
USSPACECOM MSEL Development Conference	E-I 05 days
USSPACECOM MSEL Synchronization Conference	E-85 days
USSPACECOM Final Planning Conference	E-75 days
Critical Cancellation Date	■
APOLLO CND EXECUTION	
Work COMMEX	E-5 days
Conduct Mini-EX	E-2 days
STARTEX	E-Day
ENDEX (Notional E+5 days)	E+5 days
APOLLO CND ASSESSMENT	
Observe/Evaluate	E-Day thru ENDEX
AAR Brief Chaired by SPJ3	E+5 days
Quick Look Report	E+30 days
AAR Briefing to USCINCSpace	E+60 days
Commander's Summary Report	ENDEX+20 days
JULLS Submission to CJCS	E+90 days
RAP Submission to CJCS	E+120 days

Table 3-9. Notional Apollo CND Planning Timeline

3.9.4. USSPACECOM/J37 Responsibilities. USSPACECOM/J37 is the focal point for USCINCSpace exercises. A member of the J37 staff will be assigned the position of Apollo CND Exercise Director. This individual will be the prime interface with all commands and agencies that plan to participate in the exercise. During the design process, an announcement message will solicit requirements, objectives, constraints and desires from participating organizations. These inputs will be used to formulate the exercise concept and scenario.

As the exercise design cycle progresses, the Joint Training Plan (JTP) training objectives will be used to baseline the exercise events which will be refined and incorporated into the Master Scenario Event List (MSEL), which serves as the basis of the Controllers Instruction (COSIN). MSELs will be validated by component, training audience and USSPACECOM directors who have responsibility for the event, to ensure minimal impact on operational systems. Once events are validated and the means of event insertion approved by J37, the Apollo CND COSIN will be published.

3.9.5. Execution and Control. Apollo CND exercise participants will react to simulated data and scripted inputs, and interact with other exercise participants based on the guidance found in existing tactics, techniques and procedures. Where procedures or real world activities preclude exercise players from actually performing the necessary actions, personnel in a Joint Exercise Control Group (JECG) will assist in simulating the required actions.

3.9.6. The USSPACECOM Exercise Director and the JECG, using the COSIN will control Apollo CND. The Exercise Director will head the JECG, and will control exercise activity to ensure training objectives are met. The JECG is the single point of contact (POC) for the coordination and execution of all exercise events. It will have members in all exercise participant control cells to provide interface and continuity. The JECG will review the COSIN prior to STARTEX to ensure there is an understanding of the impact of exercise MSELs on real world events that may occur during Apollo CND. The JECG Exercise Director is the final authority for adding, modifying, or deleting exercise events.

3.9.7. Exercise Assessment. Apollo CND is designed to prepare joint war-fighting commands and staff agencies to perform their Computer Network Defense responsibilities. An essential part of this process is an assessment plan that provides the capability to evaluate the results of operations and exercises and make informed decisions on resource allocation, training requirements, and operational readiness. The USSPACECOM JTP is the starting point for Apollo CND. It details Apollo CND training audience, standards and exercise objectives that will be assessed. Figure 3-9 contains a flow diagram that depicts the assessment process.

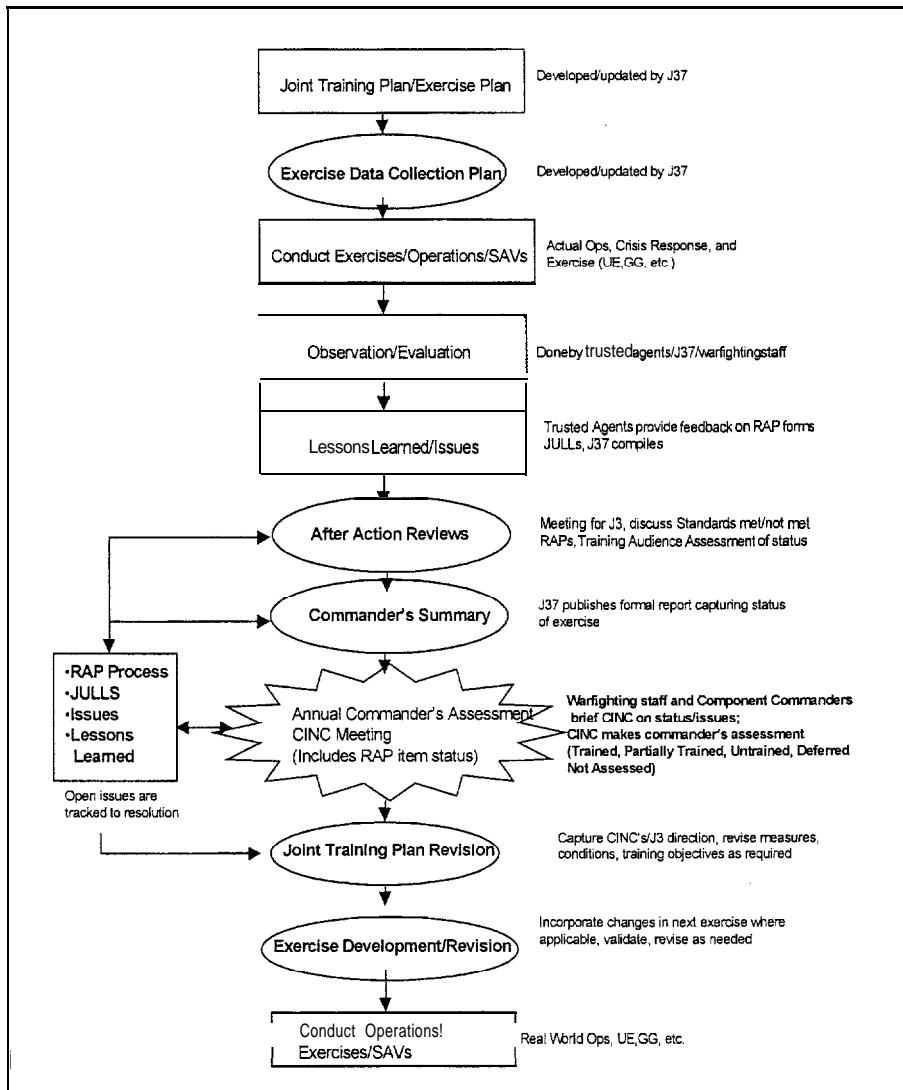


Figure 3-6 Exercise Assessment Process

3.9.8. Collection Management Plan. A Collection Management Plan (CMP) will be developed for Apollo CND that details how the information/observations required by the training objectives will be collected. It will provide structure to the data collection process by using checklist formats to ensure completion of the collection process. The CMP will be used by trusted agents (TAs) and JECG members to accurately collect the data during the exercise.

3.9.9. Observations generated by the training audience will be submitted on Remedial Action Project (RAP) data sheets. There are two types of inputs - lessons learned and issues, as described in CJCSM 3500.03. Submissions should be made as soon as possible after the observation. Related observations will be combined with prior submissions by J37. Completed Collection Management Plans (CMPS) and training

audience observation worksheets (RAPs) will be collected by J37 and used to produce a Commander's Summary.

3.9.10. After Action Review, The Apollo CND After Action Review (AAR) will be facilitated by the J3, J3V, or J37 designee. The review will be conducted with all agencies and personnel participating in the exercise. The AAR will focus on four to seven major issues, and provide the commander and training audience with the data and information needed to assist in the evaluation of the audience's training proficiency.

3.9.10.1. The AAR plan is based upon exercise objectives, commander's guidance, joint training objectives, training audience, training methods, duration of the event, level of distribution of the event, personnel and equipment available.

3.9.10.2. Commanders are required to evaluate all training events to capture training audience proficiency. The AAR process ensures that the design of joint training events provides opportunities for observations, and that data is generated, captured, and correlated to each training objective.

3.9.10.3. The AAR process provides the commander the data to conduct issue identification and readiness reporting as appropriate during the JTS assessment phase.

3.9.11. Commander's Summary, This summary is a synopsis of the training event, and provides data and information related directly to each training objective. While the AAR focuses on four to seven major issues, the commander's summary report is the mechanism to provide an assessment of all training objectives. It will be completed within 20 days of the completion of Apollo CND. The Commander's Summary will include the standards met as well as those not met, an update of RAP issues, and an assessment of training audience status based on the standards being met or not. The report will be sent to all training audiences, each directorate, and the CINC.

3.9.12. Joint Universal Lessons Learned. Joint Universal Lessons Learned (JULL) will be consolidated by J37 for release by the J3. A JULL is a technique, procedure or work around that allowed the task to be accomplished to standard based upon an identified shortcoming or deficiency within a specific command or circumstance which may be applicable to others in similar circumstances.

3.9.13. Remedial Action Project. Remedial Action Project (RAP) items will be collated, analyzed and synthesized by members of the RAP working group IAW Unified Instruction 1 O-43, *USCINCPAC* Remedial Action Project (RAP) Program, dated 1 April 1998. The Commander's Summary and CJCS-level RAPs will be prepared by J37 for release by the J3.

3.10. **Global Partnering.** USCINCPAC will work through the regional CINCs to negotiate effective CND policy with their respective foreign governments that compliment and strengthen DoD and National CND. By promulgating CND policy and standards for day-to-day operations, exercises, wargames, and contingency and crisis operations, USCINCPAC will advocate for doctrinal standards necessary for Regional CINCs to enjoin allies as part of a common CND operational methodology.

USSPACECOM J59, as focal point for CND/CNA plans, policy and doctrine, will advocate for doctrinal standards and work will with regional CINCs to negotiate diplomatic policy memoranda of agreement/understanding, and ROEs for attribution in dealing with countries where CNA/intrusion is not illegal.

Section 4 - SUPPORT TO OPERATIONS

4.0. Support To Operations. This section provides brief descriptions of Headquarters USSPACECOM staff elements support to CND mission operations. Functional areas discussed include legal; manpower and personnel; intelligence; logistics; plans and policy; command, control and communications; and public affairs. Additional information on USSPACECOM staff organization and tasks is provided in Annex 1, CND CONOPS: USSPACECOM Internal Organization and Tasks.

4.1. Legal. Timely and accurate legal advice is a prerequisite to successful CND operations. USSPACECOM/JA will be engaged in a variety of issues ranging from policy and doctrine development to resolving issues arising out of actual mission operations.

4.1 .1. SJA Policy and Doctrine Support. USSPACECOMNA will work closely with J59 to advocate for CND policy. The policy must reflect the law, to the extent that requirements exist in current law. Where the law is not specific on CND matters, USSPACECOM will seek to influence the manner in which the relevant body of law evolves. It is imperative that USCINCSpace articulate and implement doctrine in a manner that is consistent with the legal norms adopted by the domestic and international community. Accordingly, the SJA will be involved in the formulation of all CND doctrine. Only through that early involvement can the legal staff adopt the forward-looking posture that is necessary to properly serve the CINC and the staff. Moreover, this involvement will permit the SJA to forge productive working relationships with other entities that are involved in shaping the law and to advocate a legal regime that acknowledges USCINCSpace's and JTF-CND's interests.

4.1.2. SJA Support to Operations. Legal advice and counsel is essential to the development of viable courses of action associated with implementation of the CND mission. USSPACECOMNA will support J39 and the JTF-CND/JA, as required, in all aspects of planning and executing the CND mission.

4.2. Manpower and Personnel Support. USSPACECOM/J1, Director of Manpower and Personnel will provide support to CND mission operations as required. USSPACECOM has requested a total of 166 positions, i.e., 122 military and 44 contractors, to accomplish the CND/CNA mission [Reference Appendix F, CND Implementation Plan (CND I-Plan)].

4.3. Intelligence Support To Operations. The ability to provide timely and accurate warning information is inherent in the USCINCSpace CND mission to protect and defend DoD computer networks. USSPACECOMN2, Intelligence Directorate, will provide USCINCSpace, CJTF-CND, and respective staff elements with intelligence support necessary to conduct the CND mission.

4.3.1. J2 Staff Responsibilities. USSPACECOM/J2F (Information Operations Branch) is responsible for intelligence support for CND mission operations and will utilize all sources and facilities within the Intelligence Community. J2F will provide timely I&W,

assessments, estimates, and predictive analysis products and information to support the protection of DoD computer networks and information systems. J2F will provide J39 a minimum of two intelligence specialists for direct imbedded intelligence support to the J39 CND/A mission team. The concept of direct, unfiltered imbedded/matrixed support to USSPACECOM/J3 operations team has demonstrated value. For the CND/A mission, this proven approach will be replicated with imbedded intelligence support to USSPACECOM/J39.

4.3.2. J2 Resources. Existing facilities and organizations that will be leveraged include: USSPACECOM Consolidated Intelligence Watch (CIW), USCINCSpace Combined Intelligence Center (CIC), JTF-CND, partnerships with DoD intelligence agencies, as well as other intelligence capabilities and information available from other CINCs and the Services. Annex 2, CND CONOPS: USSPACECOM Intelligence Support to CND Operations provides detailed information on intelligence support for the CND mission. Annex 2 describes USPACECOMN2 plans and processes for intelligence support in these areas:

- a. Collection Management
- b. Priority Intelligence Requirements (PIR)
- c. Signals Intelligence, Human Intelligence, Imagery Intelligence, Measures and Signature Intelligence, and Open Source Intelligence.
- d. Counter Intelligence
- e. Foreign Disclosure
- f. Intelligence Community Partnerships
- g. Intelligence Oversight
- h. SCI Systems

4.4. Logistics. The Director of Logistics, USSPACECOM/J4, will provide logistics and contracting support for HQ USSPACECOM in support of the CND mission. CINCS, components, and subordinate units are responsible for logically supporting their operations in accordance with service directives. These organizations will plan and execute movement of personnel and equipment as required. USPACECOMN4 will provide guidance and assistance, including working any TPFDD, contracting support or any other issues **as** required. In addition, the J4 will provide comments and coordination on any new acquisition programs supporting the CND/CNA mission to ensure the system is logically supportable.

4.5. Plans and Policy. USCINCSpace will provide operational advocacy for all matters involving computer network defense of the Defense Information Infrastructure (DII). USSPACECOM/J5, Director of Plans, will provide support to the CND mission with responsibilities for plans, policy, requirements, and doctrine.

4.5.1. J5 Staff Responsibilities. USSPACECOMN59, CND/A Plans, Policy and Strategy Division, will provide expertise and focus on CND ((and later CNA) issues. Within the J59 division, two branches are envisioned: one to focus on computer network defense and one to focus on computer network attack issues. Specific capabilities and expertise will be provided as follows:

4.5.1 .1. Policy Development. J5 will provide integrated USSPACECOM staff support for all policy issues related to CND mission.

4.5.1.2. Programming and Budget Analysis. J5 will manage all USSPACECOM budgetary issues associated with JTF-CND and USCINCSpace inputs to the DoD Program Objective Memorandum (POM) and all other DoD programming activities.

4.5.1.3. Requirements Development. J5 will provide centralized management of all USSPACECOM operational requirements for CND/A programs. In addition, expertise will be provided concerning operational requirements for changes or additions to national systems architectures and capabilities in support of the CND/A mission. J5 will ensure USCINCSpace operational requirements are properly advocated for successful accomplishment of US military operations.

4.5.1.4. Systems Development. In addition its current requirements mission, J5 will also provide requirements expertise for new and emerging CND/A systems. The ability to closely follow development of CND/A mission programs/systems will streamline development of USCINCSpace operational requirements.

4.5.1.5. Integrated Priority List (IPL) Management. J5 will provide management expertise for CND/A issues with respect to USCINCSpace IPL process.

4.5.1.6. Deliberate Plan Development. J59 will provide J39 two Deliberate Plans Officers (one for CND mission plans and later one officer for CNA mission plans). The concept is to imbed J59 expertise in the deliberate planning process with J39 CND/A mission team to provide USCINCSpace with validated deliberate plans for employment of CND (and later CNA) mission capabilities. The concept is to produce and maintain CND/A plans to ensure CND/A missions are fully integrated into all US military operations.

4.5.1.7. Wargames/Exercises/Strategy. J59 will provide USCINCSpace and JTF-CND expertise on national security and national military strategy. The CND/A mission areas are relatively new and a key sub-component of joint vision (See JV 2010) to ensure U.S. information superiority. Considerable effort will be applied to ensure USSPACECOM CND/A mission capabilities are integrated into U.S. national strategies.

4.5.1.8. Allied and Agency Liaison. J5 will provide USSPACECOM expertise and focus on issues associated with liaison with US allies and U.S. government agencies. J5 will develop USCINCSpace advocacy related to diplomatic policies and seek to establish memorandums of agreement associated with CND/A with non-DoD government entities, the civil sector, and allies and foreign governments.

4.5.1.9. Doctrine Development. J5 will provide integrated support and advocacy for the development of DoD CND doctrine.

4.5.1.10. Guard/Reserve Augmentation. J5 will coordinate the establishment of an integrated joint CND/CNA reserve component in support of USSPACECOM's CND/CNA mission. Guard and reserve forces provide trained units and individuals to support the wide range of operations associated with performance of the CND/CNA mission. These individuals provide unique skills in carrying out the day to day information operations (IO) activities and relieving active duty personnel from routine staff commitments during crisis situations. Integrating the joint CND/CNA components as an essential participant, across the spectrum of USSPACECOM's IO, is the optimum course of action to ensure a robust flexible CND/CNA mission capability for the command and for the nation.

4.5.1.11. Education and Training. J5 will develop an Education Center of Excellence with academia for CND education and training, career development and professional growth. As the Command focal point for academia relationships, USSPACECOM J59 will ensure the Colorado Springs Information Technology Center of Excellence for training and education incorporates USSPACECOM J37's CND education and training standards and requirements.

4.6. Command, Control, and Communications. USCINCSpace and JTF-CND will receive technical advice and support for the CND mission from USSPACECOM/J6, Director of Communications and Computers. USSPACECOMNG will ensure accurate CND capabilities are integrated into deliberate and crisis planning documents. Each of these staff directorates will provide inputs through their representatives dedicated to the CND mission who reside in J39.

4.6.1. J6 Responsibility for Information Assurance (IA). In addition to supporting the CND mission, USSPACECOM/J6 will continue to execute existing responsibilities to provide USCINCSpace Information Assurance (IA) functions, capabilities and technical support to USCINCSpace space components and missions. The important IA (and related CIO/Chief Information Officer) responsibilities for internal space mission areas should not be confused with new and different range of J6 responsibilities for the global USCINCSpace CND mission. Existing IA responsibilities for space missions are not addressed in this CND CONOPS.

4.6.2. J6 Staff Responsibilities for CND Mission Support

4.6.2.1. CND Operations Support Branch. USSPACECOMNG will provide technical expertise in direct support of CND mission operations. The following activities will be conducted in support of operations:

4.6.2.2. Coordinate and assist planning efforts for development of a Common Operating Picture (COP) for DoD such as the current IA COP (a C2 system with an enhanced situational awareness capability)

4.6.2.3. Provide technical advice and coordination on legal reviews, standing rules of engagement (SROE) relationships, and proposed legislation dealing with operational issues that support DoD CND operations.

4.6.2.4. Assist USSPACE/J3/J5 in establishment and advocacy of CND SROE, operational policy, standardized JTF/Service event/incident thresholds, mission level requirements, intelligence requirements, and development of standardized certification, training, and reporting

4.6.2.5. Provide USSPACECOMIJ3 technical assistance during development of all CND COAs and plans on CND operations, to include actions required to restore networks to operational status.

4.6.2.6. Integrate, evaluate and assist in deconfliction of DoD defensive computer network actions and activities.

4.6.2.7. Assist USSPACECOM/J3/J5 planners to develop overarching implementation strategies for layered defense for the DII, to include integration and technical deconfliction of C/S/A CND inputs.

4.6.2.8. Assist the regional CINCs with the integration of CND into their exercise plans by advocating the development of war games and applicable modeling and simulation tools to provide a means to more realistically evaluate DII CND procedures.

4.6.2.9. As required, represent USCINCSpace and JTF-CND in technical matters concerning DoD CND to organizations such as the Defense Information Systems Agency (DISA), Joint Staff, the Intelligence Community (IC), National Infrastructure Protection Center (NIPC), law enforcement, and other US government agencies.

4.6.2.10. Coordinate with other C/S/A on issues involving required protective measures and standards, technical and readiness standards, necessary for effective DoD CND.

4.6.2.11. Advocate and support technical development of an integrated DII CND strategy.

4.6.2.12. Assist USSPACECOMN3 in the development and maturation of DoD CND standardized reporting and network operational assessments.

4.6.2.13. Support USSPACECOM/J35/J39 development of standardized readiness reporting as part of the Joint Monthly Readiness Review (JMRR).

4.6.2.14. As required, support USSPACECOM/J3 and participate in employment of DOD red teams and computer network vulnerability assessment team activities.

4.6.2.15. Provide USSPACECOMN3 technical advice on required protection measures, methods to resolve unique C/S/A network protection issues, and technical support for operational advocacy for DoD-wide CND priorities.

4.7. Space Operations Center (SPOC) Support Branch. USSPACECOM/J6 will provide technical expertise in direct support of real-time CND mission operations being executed from USCINCSpaceISPOC (USSPACECOM/J36). The following activities will be conducted in support of J36/SPOC activities:

- 4.7.1. Provide USSPACECOM/J36 technical advice in the conduct of CND mission operations.
- 4.7.2. Assist USSPACECOM/J36 in providing a flexible and responsive command and control (C2) structure for execution of CND mission operations.
- 4.7.3. Assist USPACECOM/J36/J39 personnel with establishment of CND mission level teleconferences, messages, SIPRNET/GCCS postings, etc.
- 4.7.4. Assist SPOC personnel in preparation of USCINCSpace directive messages to implement DoD CND response actions.
- 4.7.5. Assist USSPACECOM/J3 with coordination of changes to DoD-wide INFOCON.
- 4.7.6. Provide timely coordination and effective communication to USSPACECOM/J6 (and J6 staff elements) on current USCINCSpace and JTF-CND global CND mission operations. Timely awareness of CND related-problems/issues allows J6 to fulfill two important responsibilities: (1) technical advice to USSPACECOM/J3, JTF-CND and USCINCSpace on global CND mission activities; and (2) internal Information Assurance (IA) for NORAD/USSPACECOM mission operations.

4.8. NORAD-SPACECOM Operations Branch. [TBD].

- 4.8.1. NORAD-SPACECOM Plans Branch. [TBD].

4.9. Public Affairs. USSPACECOM/PA provides public affairs support to the CND effort in direct coordination with the Office of the Assistant Secretary of Defense for Public Affairs (OASD/PA) and the PA offices of regional and functional CINCs. PA communications strategy will include scheduling and coordinating interviews with USSPACECOM's senior leaders and technical experts on CND; preparing and distributing timely news releases; preparing products such as fact sheets or background information; and issuing period public affairs guidance (PAG). All materials will emphasize key messages about CND. Public releases will be posted on USSPACECOM's public web site and/or the SIPRNET, as appropriate.

HEADQUARTERS, U.S. SPACE COMMAND
250 S Peterson Blvd, Suite 116
Peterson AFB, CO 80914-3010
1 September 1999

Annex 1 USSPACECOM Internal Organizations and Tasks, USSPACECOM Computer Network Defense (CND) Concept of Operations (CONOPS)

TABLE OF CONTENTS

INTRODUCTION	2
1.0 Directorate of Personnel (J1)	2
1 .1. Manpower, Organization and Plans Division (JIM)	3
2.0 Directorate of intelligence (J2).	3
3.0. Directorate of Operations (J3).	3
3.1. Readiness Division (J-35)	5
3.2. Current Operations Division (J36)	5
3.3. Exercise, Training and Education Division (J37)	9
3.4. Counterspace and Information Operations Division (J39).	11
4.0. Directorate of Logistics (J4)	20
5.0. Directorate of Plans (J5)	20
5.1. CND/A Plans, Policy and Strategy Division (J59)	20
6.0. Directorate of Command Control Systems (J6)	25
6.1. J6 Mission	27
7.0. Staff Judge Advocate (SJA)	34
8.0. Public Affairs (PA)	34

List of Tables

Table D-1. J1Tasks	2
Table D-2. J3 Tasks	3
Table D-3. J5 Tasks	22
Table D-4. J6 Tasks....	25
Table D-5. Other CINC's Staff Tasks	34

HEADQUARTERS, U.S. SPACE COMMAND
250 S Peterson Blvd, Suite 116
Peterson AFB, CO 80914-3010
1 September 1999

USSPACECOM Computer Network Defense (CND) Concept of Operations (CONOPS)

Annex 1: USSPACECOM Internal Organization and Tasks

Introduction. This Annex provides the mission statement and tasks associated with the CND mission for internal HQ USSPACECOM Directorates, e.g., J2, J3, etc., and Divisions, e.g., J2F, J39, etc. The purpose is to provide the USSPACECOM staff with an understanding of the tasks assigned to their directorate and division. A matrix, mapping the tasks against the directorate's divisions and brief text explanation of the associated tasks, is provided.

NOTE. In the matrixes, the "P" represents tasks which the division holds primary responsibility. The "S" represents tasks which the division has secondary or collateral responsibilities. In addition, primary and secondary tasks are not necessarily conducted only within the domain of the division(s) identified. Many HQ USSPACECOM staff activities are integrated efforts with portions conducted by all divisions. In addition, the J39 division will be matrixed with personnel from J2, J3, J5, and J6. Tasks within the J39 column may appear to be more applicable to the J2, J5, and J6 organizations; however, they will be resident within the J39 division.

1.0. Directorate of Personnel (J1). The Manpower, Organization and Plans Branch (J1 M) will: review plans, publications, and policy documents for manpower and personnel impact; provide exercise/contingency support; develop manpower requirements change packages; conduct manpower reviews; respond to OSD, Joint Staff and command manpower taskings; and, represent manpower issues during the POM and IPL cycles.

Task	J1M	Comment
Plans management (manpower and personnel)	P	
Exercise/contingency support	P	
Joint publications & policy documents review	P	
Manpower Requirements Change Package development	P	
Manpower reviews, studies and reductions	P	
OSD, JS, Command and Directorate manpower taskings	P	
Represent manpower issues during POM and IPL Cycles	P	

Table D-I. J-I Tasks

1.1. Manpower, Organization and Plans Division (JIM).

1.1.2. Mission Statement. Review plans, publications, and policy documents for manpower and personnel impact; provide exercise/contingency support; develop manpower requirements change packages; conduct manpower reviews; respond to OSD, Joint Staff and command manpower tasking; and, represent manpower issues during the POM and IPL cycles.

1.1.3. Task Descriptions.

1.1.3. 1. Review and write personnel annexes to OPLANs and EXPLANS

1 .1.3.2. Participate in exercises and contingencies and provide manpower and personnel guidance and support.

1 .1.3.3. Review joint publications and policy documents for manpower and personnel impact.

1 .1.3.4. Develop Manpower Requirements Change Packages for submission to the Joint Staff.

1.1.3.5. Conduct manpower reviews, studies and reductions as directed by OSD, Joint Staff or the CINC.

1 .1.3.6. Respond to OSD, Joint Staff, Command and Directorate manpower taskings

1 .1.3.7. Represent command on manpower issues during POM and IPL cycles in various meetings and forums.

2.0. Directorate of Intelligence (J2). (Ref annex 2.)

3.0. Directorate of Operations (J3). SP/J3 will operationalize, organize, advocate, and coordinate CND exercises across C/S/As. They will advocate standardized training and education requirements, and (in conjunction with N/SPAN) coordinate CND modeling and simulation efforts. In addition, they will produce a Joint Monthly Readiness Review for the DOD CND mission and force structure. This will be based in large measure on inputs from the JTF-CND, but also on frequent interaction with C/S/As.

Task	J35	J36	J37	J39	Comments
JMRR development	P				
Current ops monitoring/crisis support		P		S	
Conduit to J3 and CINC for ops issues		P		S	
LNO support for CND		P			
Task	J35	J36	J37	J39	Comments
Develop/coordinate exercises			P		
Primary Command POC for CND				P	
Reachback for FOB/CAT/BS for:				P	
- OPORD Development				P	
- COA development (respond/restore functions)				P	
- Mission operations integration, coordination				P	
Develop and coordinate deliberate and crisis action plans and supporting CND annexes				P	Assisted by J2, J5, J6
Evaluate COA effectiveness, and identify changes to priorities, pre-planned TTP, and capabilities.		S		P	
Develop and coordinate ROE, Uls, CONOPS, INFOCON guidance, reporting processes, TTPs, etc				P	
Coordinate with C/S/As; ID role with national security interests				P	
Develop EEIs for PIR development				P	
Deconflict Red Teams				P	
Develop partnerships and relationships with non-DOD agencies, private sector, and foreign, allies/coalition partners for integrating responses to CNA				P	
Interface with Law Enforcement Agencies (Military and Civilian)		P		S	
Deconflict Offensive and Defensive computer network activities		P		S	
Coordinate DOD INFOCON changes		P		S	

Provide C2 structure			P	
Advocate for Common Operating Picture (COP)			S	P = J6O
Coordinate CND current operations with mission partners (Govt., civil, industry, academia)	P		S	
Provide inputs to Joint Mission Essential Task List (JMTEL)		P	S	
Advocate standardized Joint training and certification requirements		P	S	
Advocate requirements for modeling/simulation tools			S	P = N/SPAN/J6

Table D-2. J3 Tasks

3.1. Readiness Division (J35).

3.1.1. Command lead for the CJCS' Joint Monthly Readiness Review (JMRR) process, the primary forum through which USCINCSpace assesses and reports his ability to execute assigned missions, including Computer Network Defense.

3.1.2. Task Description. Office of Primary Responsibility for USSPACECOM's readiness assessment process in support of the JMRR process.

3.1.2.1. Develop process for assessing and reporting global CND operational readiness through the JMRR process.

3.1.2.2. Work with Joint Staff, JTF-CND and other Unified Command staffs to develop CND assessment criteria and reporting procedures to support USCINCSpace's mission of protecting the DII.

3.1.2.3. Develop metrics for assessing DoD-wide CND operational readiness according to mission responsibilities.

3.1.2.4. Obtain readiness inputs from JTF-CND (and others as required). Analyze data, and determine readiness status of DII.

3.1.2.5. Report CND-related deficiencies against the applicable joint readiness functional area(s) in USCINCSpace's JMRR message.

3.1.2.6. Integrate CND into the command's readiness assessment process.

3.2. Current Operations Division (J36)

M

3.2.1. Space Operations Center (SPOC). Provides continuous (24x7) capability and develops interactive relationships with other CINC's operations centers. Daily interactions will provide enhanced situational awareness of current military operations and exercises, and will satisfy space support requirements via CND watch officers in the SPOC. Additionally, the future operations branch of J36 will focus on operations and planning 24 hours to 2 weeks in the future mapping out planned space and CND support requirements.

3.2.2. Task Descriptions

3.2.2.1. Current operations monitoring/crisis support.

a. Provide 24 hour-a-day operations oversight and support to the JTF CND via the SPOC. Provide updates to JTF-CND on real world military operations, exercises or other information to help with situational awareness pending OPLAN executions, etc.

b. Monitor the status of the DII:

1. Collect and monitor daily operations reports, threat advisories, incident reports, etc.

2. Update the USSPACECOM CND web page and/or operations/intelligence briefing of changes to DoD network status.

c. Provide crisis action support to the HQ USSPACECOM staff and the JTF CND as required:

1. Assist the JTF CND to check with Red Teaming agencies and organizations to eliminate Red Teaming as a possibility for the source of the report(s).

2. Determine if USCINCSpace should direct a change to the DOD INFOCON level.

3. Coordinate with other non-DoD government organizations, industry, academia, etc. to share threat advisories, collect data on similar activities and request support for DoD CND response/restoral activities.

4. Assist the JTF CND in recommending COAs for CINC assessment to the threat.

5. Assist the JTF CND/GNOSC in selecting and/or modifying a COA to respond to the threat.

6. Coordinate the approval of restoral and prevention directives with the J3/USCINCSpace. (Note: the CJTF will also have the authority to report directly to USCINCSpace or J3, directly.)

7. Prepare (or assist the JTF CND in preparing) and issue mission orders directing actions in response to an intrusion/attack or threat of an intrusion/attack.
 8. Monitor the success/status of restoral actions.
 9. Provide inputs to after-action analyses to recommend where improvements are required to current detecting and response processes, directives, etc. at all command levels within the DoD CND process.
- 3.2.2.2. Conduit to J3 and CINC for ops issues
- a. Provide the primary interface between the J3/USCINCSpace and the daily operational activities of the SPOC and the JTF CND.
 - b. Provide notification of reportable changes to DII CND status.
 - c. Staff intrusion/attack assessment recommendations, COA responses, and INFOCON changes in response to intrusion/attack.
- 3.2.2.3. Assist in the development and modification of COAs and the assessment and selection of COA options during crisis operations.
- 3.2.2.4. Liaison Officer (LNO) support for CND.
- a. Provide LNO support to C/S/As, similar in concept to the Space LNOs who provide space support to the regional CINCs .
 - b. Develop and implement a resource and response structure that can effectively deliver CND support to all C/S/As as required.
 - c. LNO support activities may include: Reach-back to USSPACECOM Staff (J39) or the JIOC for additional CND support.
 1. Support to deliberate planning activities.
 2. Support to crisis action planning/crisis operations.
 3. Coordinate technical support and operational assessments.
 4. Provide feedback for after-action reports to identify changes to operational processes, pre-planned TTP, and CND capabilities.
 5. Promulgate and clarify CND policy, doctrine, guidance, standards, etc.
 6. Provide CND exercise planning support and participation.
- 3.2.2.5. Evaluate COA effectiveness, and identify changes to priorities, pre-planned TTP, and capabilities,

- a. In support of crisis operations, the SPOC and JTF CND will review and select pre-existing restoral plans/COAs. Selection criteria could include:
 - 1. The impact that implementation of the COA will have to current and planned mission operations.
 - 2. Resource and time requirements to implement a restoral action/COA
 - 3. The weighting of the impact between responding with a restoral plan/COA vs. allowing an attack to continue in order to gather intelligence or evidence for prosecution.
- b. Depending on the restoral plan/COA selected, oversee the modification of existing TTP, if required.
- c. Perform an after-action review of COA and TTP effectiveness that may indicate where changes are required to more effectively combat a future CNA threat.

3.2.2.6. Coordinate with JTF-CND concerning interface with Law Enforcement Agencies (LEAs) (Military and Civilian).

- a. Assist the JTF CND, establish and maintain an operational interface with military and civilian LEAs as mission planning and operations require.
 - 1. DoD LEAs include Counter-Investigation Division (CID), the Office of Special Investigation (OSI), Naval Criminal Investigative Service (NCIS), and Defense Criminal Investigative Service (DCIS).
 - 2. Civilian law enforcement activities will be coordinated via the FBI's National Infrastructure Protection Center (NIPC).
 - b. It is important to normalize operations with these mission partners so efficient support is mutually provided during crisis operations. This is particularly important since portions of the DII ride on non-DoD networks.
 - c. Coordination activities with military and civilian LEAs may include:
 - 1. Notification of incidents that may cross the DII into the NII.
 - 2. Exchanges on the status of ongoing investigations and requirements for further information collection (vs. the need to restore operational capability immediately).
 - 3. Known vulnerabilities which affect the NII.
 - 4. Information on patches and actions to defend, contain, or restore the DII.

3.2.2.7. Deconflict Offensive and Defensive computer network activities.

- a. Maintain situational awareness of ongoing defensive and offensive DoD network operations. Comprehensive offensive/defensive situational awareness may only be available at higher security levels when conducted within SPOC operations. If so, deconfliction will be the responsibility of appropriately cleared personnel within J36 and/or J39.
- b. Deconflict defensive and offensive planning activities so offensive operations do not nullify an ongoing or planned defensive operations. Evaluate situations and determine whether creating an integrated activity could potentially negate competing CND/CNA/CNE activities, and vice versa.
- c. Facilitate synergy between CND and CNA ensuring protection of US computers and networks against known attacks/intrusion methodologies.

3.2.2.8. Coordinate DoD INFOCON changes.

- a. Based on JTF CND recommendations, determine whether a current situation (or potential situation) warrants a change in the DOD-level INFOCON.
- b. If a decision is made to recommend USCINCCSPACE declare an INFOCON change, staff the recommendation through the J3 to USCINCCSPACE. (time permitting)
- c. If an INFOCON change is approved, develop with/or assist the JTF CND (as required) implementing the directive on behalf of USCINCCSPACE.
- d. If required, assist the JTF CND in tracking and reporting the responses of the C/S/As as they accomplish the tasks associated with changing the DoD INFOCON level.
- e. Continue to monitor the situation that initiated the INFOCON change requirement, and recommend downgrading the level when practical.

3.2.2.9. Coordinate CND operations with mission partners (government, civilian, industry, and academia).

- a. If responding to an operational incident, support the JTRF-CND to coordinate notification and support activities with mission partners (within the scope of operational security restrictions).
- b. Help identify mission partners who could be affected by the threat or by the actions directed by the CJTF-CND or CINCSPACE.
- c. Provide insight to the JTF-CND into operations or activities of mission partners to help deconflict CND actions with their operations
- d. Normalize operations with these mission partners so efficient support is mutually provided during crisis operations. This is particularly important since portions of the DII ride on commercial networks.

e. As opportunities arise, establish and develop similar relationships with allied forces, while protecting national and commercial security and interests as required.

3.3. Exercise, Training, and Education Division (J37)

3.3.1. USSPACECOM/J37 Division. The Joint Training, Exercise and Education Division is the office of primary responsibility for the USCINCSpace Joint Training Program. With support of other USSPACECOM offices and elements, J37 performs the following functions:

- a. Develops and maintains the USCINCSpace JMETL.
- b. Develops and publishes the annual USCINCSpace Joint Training Plan.
- c. Maintains the USSPACECOM Joint Training Schedule.
- d. Develops, executes, and evaluates the effectiveness of specific training events.
- e. Implements the USSPACECOM Training Assessment Program, including the Joint After Action Reporting (JAAR) Program, the Joint Lessons Learned (JULLS) Program, and the Remedial Action Project (RAP) Program.
- f. Coordinates joint training issues and requirements for specific training events with other combatant commands, joint agencies, and component commands.
- g. Coordinate all Red Team related support during exercises involving participation by USSPACECOM and its components.
- h. Represents USCINCSpace with the Joint Staff on all joint training issues (joint training policy, procedures, funding and resources, and other support).
- i. Provides guidance to component commands in their development of supporting component mission essential tasks lists, training plans, training events, and assessments.

3.3.2. Tasks Description.

3.3.2.1. Develop/coordinate exercises.

a. Contribute to efficient, coordinated responses to real world intrusions/attacks by sponsoring CND-related exercises that practice and refine CND processes and operational interfaces at all levels of command.

b. Coordinate with all C/S/As to ensure that CND threats and scenarios are incorporated into joint and multi-command exercises.

c. Assist in developing objectives and scenarios to rehearse specific threats, operational impacts, and responses.

d. Determine requirements for C/S/A conduct/participation in CND-related exercises (including the JTF CND and HQ USSPACECOM staff).

3.3.2.2. Advocate standardized Joint training and certification requirements.

a. Establish a process and criteria for recommending minimum DOD training and certification requirements required to conduct advanced protection, monitoring, detection, restoral activities and response for CND mission operations.

b. Advocate CND operational awareness and technical training requirements to service “schoolhouses” and other DOD training activities where possible (i.e. within DOD agencies for incorporation into computer network technical training courses and other courses as applicable).

c. Advocate CND operational awareness and technical training requirements to non-DOD government organizations, industry, and academia. Coordinate with these organizations in developing common training and certification requirements

3.4. Counter Space and Information Operations Division (539).

3.4.1. A matrixed organization, integrating and leveraging J2, J3, J5, and J6 expertise, that serves as the primary HQ USSPACECOM POC for the DoD CND mission.

Develops and coordinates OPLANS, CONPLANS, contingency plans and supporting CND annexes. Coordinates and integrates USSPACECOM support to C/S/As and allied operations for the DoD CND mission. Provides guidance to the JTF-CND in the form of unified instructions, CONOPs, ROEs, and other documentation as required. Coordinate mission support and integrate the efforts of the C/S/As to provide an operational focus to the overall DoD CND mission. J39 matrixed personnel will interact frequently with their parent USSPACECOM J-staff directorates to ensure consistency of support to the DoD CND mission.

3.4.2. Task Descriptions.

3.4.2.1. Current operational monitoring/crisis support.

a. Maintain situational awareness of the status and CND-related activities of the DoD DII.

1. Collect and monitor daily operations reports, threat advisories, incident reports, etc.
2. Assist the SPOC in notifying the USSPACECOM senior staff of changes and issues regarding the status of the DoD DII.
3. In coordination with the SPOC, monitor and collect I&W for indications of possible threatening activities.

b. Provide crisis action support to the HQ USSPACECOM staff, the SPOC, and the JTF CND as required:

1. Confirm and correlate incident reports with the reporting C/S/A.
2. Poll other C/S/As for similar indicators from those provided on incident report(s).
3. Determine the ops impact of the intrusion/attack on the affected C/S/A(s).
4. Determine if USCINCSpace should direct a change to DoD INFOCON level and make recommendation.
5. Coordinate with other non-DoD government organizations, industry, academia, etc. to share threat advisories, collect data on similar activities and to request support to DoD CND response/restoral activities.
6. Assist the JTF CND in recommending a CINC assessment to the intrusion/attack.
7. Assist the JTF CND/GNOSC in selecting and/or modifying a COA to respond to the threat.
8. Develop Standing Rules of Engagement (SROE) for CND operations.
9. Work with the affected C/S/A(s) to determine the impact of implementing the selected COA. Determine collateral impacts to other C/S/As if required to implement preventative measures in response to the intrusion/attack.
10. Coordinate the approval of restoral and prevention directives with the J3 and USCINCSpace. (Note: the CJTF will also have the authority to report directly to USCINCSpace via the J3.)
11. Assist the SPOC or JTF CND in preparing) and issue mission orders directing actions in response to a intrusion/attack or the impending threat of a intrusion/attack.
12. Monitor the success/status of restoral actions.
13. Prepare event after-action analyses to determine where improvements are required to current detecting and response processes, directives, etc. at all command levels within the DoD CND process.

3.4.2.2. Conduit to J3 and CINC for ops issues.

- a. Provide a support interface between the J3/ USCINCSpace and the daily operational activities of the SPOC/J36 and the JTF CND.

b. Provide notification of reportable changes to DII CND status. Staff intrusion/attack assessment recommendations, COA responses, and INFOCON changes in response to intrusion/attack

3.4.2.3. Staff Assistance (SA) to JTF CND and conduit to C/S/A for operational issues.

a. Provide timely support to JTF CND and C/S/As as required. Most operational-level interface with the C/S/As will occur via the JTF CND and SPOC. However, if the JTF CND is resource constrained, or required activities are outside the scope of the CJTF's authority, J39 may provide the conduit for coordinating operational issues with C/S/As, including the following:

1. Provide assistance to the SPOC/JTF CND information collection and ops assessment process.
2. Facilitate interfaces between the JTF CND, SPOC, and C/S/As with non-DoD government organizations, industry, academia, etc., such as technical support for crisis operations or computer network protection measures. Assist in the development and modification of COAs and the assessment and selection of COA options during crisis operations.
3. Streamline processes for conducting and integrating CND activities at all levels of operations.
4. Provide SROE for CND operations.
5. Assist the SPOC/J36 to collect and provide Priority Intelligence Requirements (PIRs) to the Intelligence Community (IC) on behalf of the C/S/As. Once submitted, track the PIRs to ensure timely response to the requestor and the rest of the CND community, if applicable.

3.4.2.4. The Command POC for CND mission.

- a. Serve as the focal point for non-real time operations and planning issues (SPOC handles real time CND mission support activities).
- b. Oversee the generation of plans, process-refinement, Unified Instructions (UIs) TTP, etc. to ensure a process-driven and standardized format for conducting CND mission operations.
- c. Develop and maintain mutual supporting relationships with mission partners, inside and outside the DoD.
- d. Support other CINCs in their development of OPLANS/CONPLANS.
- e. Develop the USSPACECOM CONPLAN for CND operations.

f. Develop/coordinate documentation to integrate the efforts of our mission partners and provide operational focus to the CND mission.

3.4.2.5. Reachback for FOB/CAT/BS

a. Assist the FOB, as required, in preparation of OPORDS and FRAGOs or other current operational guidance to the JTF-CND.

b. COA Development (restore/respond functions):

1. Oversee COA development and modification during both the deliberate planning and crisis action planning processes.

2. The JTF CND will be the primary OPR for the development of CND COAs; J39 (and the SPOC) will provide review and refinement from a mission operations perspective.

3. Direct the selection of a COA in response to a intrusion/attack threat (based on recommendations from the JTF CND and SPOC).

c. Mission operations integration, coordination. Support the conduct of daily mission operations at the SPOC and JTF CND as required. Activities may include facilitating interfaces with mission partners and non-DoD organizations, coordinating assessments and directives to the J3 and USCINCSpace, and assisting in the development of processes, standards, directives, etc. to guide the execution of the CND mission.

3.4.2.6. COA Effectiveness, Changes to Priorities, Pre-planned TTP, and Capabilities.

a. In support of crisis operations, assist the SPOC and JTF CND in reviewing and selecting pre-existing restoral plans/COAs. Selection criteria could include:

1. The impact that implementation of the COA will have to current and planned mission operations.

2. Resource and time requirements to implement a restoral action/COA

3. The weighting of the impact between responding with a restoral plan/COA vs. allowing an attack to continue in order to gather intelligence or evidence for prosecution.

b. Depending on the restoral plan/COA selected, oversee the modification of existing TTP, when required.

c. Perform an after-action review of COA and TTP effectiveness that may indicate where changes are required to more effectively combat a future CNA threat.

3.4.2.7. Develop and Coordinate SROE, UIs, CONOPS, INFOCON Guidance, Reporting Processes, TTPs

a. Provide standing guidance under which all CND mission partners will operate and define activities for CND operations in the form of ROE, UIs, CONOPS, INFOCON guidance, reporting processes, and TTPs.

1. Guidance must be specific for anticipated CND activities. The guidance must consider the scope of authority and roles and responsibilities of all associated organizations. However, developers of the standing guidance must also be prepared to modify operational guidance, if required, to provide tailored direction as a potential CNA situation develops.

a. Closely coordinate products (perhaps even jointly develop) with the JTF CND ensuring technical and operational accuracy.

b. Develop and implement thresholds or “trigger points” that require the JTF CND/SPOC to take immediate CND actions.

c. Routinely review USSPACECOM-generated guidance

3.4.2.8. Coordinate with C/S/As (identify USSPACECOM’s role with respect to national security interests).

a. Provide support to C/S/As’ planning, operations, and support activities.

b. Support crisis operations activities, select and coordinate CND response options/COAs, and coordinate technical support from other support sources, such as non-DoD agencies, and commercial and academia support centers.

c. Identify the roles and responsibilities of USSPACECOM and the JTF CND as elements of the national infrastructure protection community.

1. Develop cooperative relationships with the implementers of national security protection concepts, particularly the NIPC, protecting the national infrastructure.

2. Influence and assist in developing concepts and national-level policy governing USSPACECOM’s role in protecting the DoD portion of information and information networks.

d. Interface with C/S/As to improve CND processes and integrate efforts across DoD.

3.4.2.9. Develop Essential Elements for Information (EEIs) for Priority Intelligence Request (PIR) development.

a. Using C/S/A and JTF CND inputs as the basis, develop core intelligence information requirements to form the basis for CNA I&W and operational assessment activities.

1. I&W reports and assessments will be “pulled” from the Intel Community IAW procedures provided for by the responsible agency.

2. J2 will coordinate with JTF CND and NIPC for domestic collection.

b. Coordinate with J2 to collect and provide Priority Intelligence Requirements (PIRs) to the Intelligence Community (IC) on behalf of C/S/As and the JTF CND as required. Once submitted, track the PIRs to ensure timely response to the requestor and the rest of the CND community, if applicable.

3.4.2.10. CND Red Team Support.

a. Provide a centralized function for monitoring Red Team requests and maintain cognizance of ongoing and planned Red Team support across the DoD.

1. USSPACECOM will not schedule all Red Team resources across the DoD. Rather, USSPACECOM will receive Red Team schedules, visit objectives, etc.

b. Assist CINCs in obtaining Red Team support, if required.

c. Identify all DoD organizations/agencies that provide Red Teams and categorize the specific nature of their capabilities/specialties.

d. Provide a consolidated process for informing C/S/As about Red Team capabilities and guidance/instructions for requesting their assistance.

e. Deconflict requests for Red Team support. Factors to consider in determining priorities for Red Team support:

1. Level of suspected vulnerability of the requestor’s networks (i.e. how critical is it for a Red Team to provide an assessment of actual network vulnerabilities).

2. Time since the last Red Team visit/assessment.

3. Operational priority of the network(s) to be evaluated.

f. Coordinate with Red Teams to ensure USSPACECOM and the JTF CND are “Trusted agents” in all Red Teaming activities and plans. This will maintain cognizance of support to exercises and other activities where Red Teaming operations could have unintentional collateral effects on other portions of the DII.

g. Upon receipt of incident and event reports, assist the SPOC and JTF CND to check with Red Teaming agencies and organizations to eliminate Red Teaming as a possibility for the source of the report(s).

3.4.2.11. Develop partnerships and relationships with non-DoD agencies, private sector, and allies/coalition partners for integrating responses to intrusions/attacks.

- a. Develop interactive partnerships with Government agencies and industry that will advance concepts for a fully integrated defense-in-depth of the DII and NII.
- b. Develop MOAs/MOU^s to define the cooperative interfaces and support capabilities between USSPACECOM and non-DoD government agencies and industry.
- c. Within the bounds of security requirements, share advisories and warnings of potential or actual intrusions.
- d. Attend conferences on information assurance-related activities and technologies hosted by other government agencies.
- e. Include representatives from other government agencies at the biannual conference hosted by USSPACECOM. Consider including in the conference schedule a segment for interchange between DoD and non-DoD agencies, the private sector, academia, and if possible, allies and coalition partners.
- f. Share TTP, support tools, and lessons learned.
- g. Consolidate training and certification requirements and courses to develop common technical skills across the spectrum of CND activities.

3.4.2.12. Interface with Law Enforcement Agencies (Military and Civilian).

- a. In coordination with the SPOC and JTF CND, establish interfaces and coordinate support with military and civilian LEAs as mission planning and operations require.
 1. DoD LEAs include CID, OSI, NCIS, and DCIS.
 2. Civilian law enforcement activities will be coordinated via the FBI's NIPC.
- b. It is important to normalize operations with these mission partners so efficient support is mutually provided during crisis operations. This is particularly important since portions of the DII ride on non-DoD networks.
- c. Coordination with military and civilian LEAs may include:
 1. Status of ongoing investigations.
 2. Notification of incidents that may cross the DII into the NII.
 3. Known vulnerabilities that may affect the NII.
 4. Information on patches and actions to defend, contain, or restore the DII.

3.4.2.13. Deconflict Offensive and Defensive Computer Network Activities. Maintain situational awareness of ongoing defensive and offensive DoD network operations.

3.4.2.14. Develop/coordinate C2 process,

a. Establish and maintain efficient processes and capabilities for command and control of CND. Some considerations for developing a C2 structure include:

1. A clear division of authorities and responsibilities for all DoD CND players
2. Coordinated and clearly documented checklists and procedures between the USSPACECOM staff, SPOC, and the JTF CND
3. Conduct/Prepare exercises and plans for a variety of threat situations and responses
4. Provide systems and processes, a combination of automated and manual, to monitor, communicate, plan, and execute CND operations at all levels of command
5. Establish ROEs for guiding, monitoring, assessing, and response actions
6. Assist in planning and providing a comprehensive common operating picture of DII systems, planning activities, and response actions to USCINCSpace, the CJTF, and other C/S/As as directed.
7. Advocate and establish standardized terminology for effectively communicating CND operations and requirements.

3.4.2.15. Advocate for Common CND C2 Architecture.

a. Provide C2 requirements for a robust and flexible C2 architecture for CND mission operations. The architecture should be able to accommodate advancements in CND/ technologies, changes in organizational structure, and modifications to CND/ related policy and doctrine.

b. C2 structure should provide for planning and execution of all USSPACECOM mission areas (CND, space, and future CNA), including a capability to quickly obtain and maintain a situational awareness of DII network configurations, status, and CND mission planning and execution activities.

c. C2 requirements should include capabilities for C/S/As to interoperate with the JTF CND and USSPACECOM conducting the DoD CND mission.

3.4.2.16. Provide J5 requirements inputs to Joint Warfare Capability Analysis (JWCA) and Joint Requirements Oversight Council (JROC) process.

Note: The source for requirements will often arise out of regular interactions with DoD CND C/S/A "customers", particularly via the LNOs. Other requirements may be

generated from after-action assessments of real world responses to intrusion/attacks, Joint Universal Lessons Learned from exercise participation, vulnerability assessments, and technological developments in network attack, intrusion detection, and attack response capabilities.

- a. Assist J5 to formulate and provide to the JWCA an overview of current capabilities for DoD C/S/As to conduct CND. Present an assessment of these capabilities, and provide feedback on behalf of the C/S/As of new capabilities requirements, for both budgets/resources and policy.
- b. Assist J5 to collect, integrate, and communicate USSPACECOM, JTF CND, and DoD C/S/A operational requirements to conduct the CND mission.

3.4.2.17. Provide J5 inputs to CND Policy and Doctrine.

- a. Assist USSPACECOMJ59 for advocating CND policy and doctrine for CND operations on behalf of DoD C/S/As.
- b. Conduct periodic reviews with J5 of existing policy and doctrine for information protection and operations to identify inadequacies in existing guidance.
 1. For example, current doctrine that focuses on Information Operations may not adequately address the role of CND in theater operations, or the role of CND as a supporting function to other facets of Information Operations.
 - c. Submit and coordinate recommended modifications to policy and doctrine to J5 for Joint Staff consideration.
 - e. If required, review J5 developed drafts for new policy and doctrine with J5 for inclusion into existing guidance, or even as a new publication, such as the Joint Publication 3-14, Space Operations Tactics, Techniques, and Procedures. (The potential for the development of new policy and doctrine may be even more likely when USSPACECOM assumes the CNA mission.)

3.4.2.18. Delegate authority to CJTF.

- a. Establish USCINCSpace scope and guidelines for CJTF CND authority to assess, direct, and execute the CND mission.
- b. Observe the flow of operational activities and identify situations where the CJTF CND is limited in authority and responsibility (or perhaps given too wide a latitude) to direct execution of CND activities. Provide recommendations to USCINCSpace to modify the scope of CJTF CND authority.
- c. It is anticipated that modifications to the scope of authority delegated to the CJTF CND will occur as the mission and relationship between USSPACECOM and the JTF CND matures.

3.4.2.19. Coordinate CND operations with mission partners (Government, civilian, industry, and academia).

- a. Once relationships are defined, J39 will coordinate crisis and non-crisis operations with mission partners.
- b. When responding to an operational incident, coordinate notification and support activities with mission partners within the scope of national and operational security restrictions.
- c. As part of non-crisis planning and support activities, assist J5 in developing MOAs and MOUs with mission partners to help formulate a defense-in-depth operational architecture and to guide the conduct of information exchange and support operations.
- d. Establish and develop similar relationships with allied forces, protecting national and commercial security and interests as required.
- e. As part of non-crisis planning and support activities, develop MOAs and MOUs with mission partners to help formulate a defense-in-depth operational architecture and guide the conduct of information exchange and support operations when real world situations develop.
- f. Normalize operations with mission partners so that efficient support can be mutually provided during crisis operations. This is particularly important since portions of the DII ride on commercial networks.

3.4.2.20. Provide inputs to Joint Mission Essential Task List (JMETL).

- a. Establish essential objectives and tasks to be performed in support of CND operations and document these in the JMETL.
- b. Use the JMETL to assist in formulating TTP.
- c. Ensure joint and multi-command exercises support JMETL objectives throughout all levels of CND operations.

4.0. Directorate of Logistics (J4). CINCS, components, and subordinate units are responsible for logically supporting their operations IAW service directives. They will plan and execute movement of personnel and equipment as required. USSPACECOMN4 will provide guidance and assistance as required, including working any TPFDD issues. In addition, the J4 will provide comments and coordination on any new acquisition programs supporting the CND mission to ensure the system is logically supportable.

5.0. Directorate of Plans and Policy (J5). SPJ5 will develop, coordinate and advocate for CND plans, concepts, policy, doctrine, Integrated Priority List, and mission-level requirements. In addition, they will assist in development and support of command

and DOD partnerships with selected industry, academia and allies, including development of the necessary memoranda of agreement/understanding (MOA/MOU).

Task	J59	J5B	J5R	J5I	J5X
Facilitate and advocate CND Policy, Doctrine, and Legislation	P	S	S	S	S
Integrate CND into War Gaming activities	P		Supported by SPJ37		
Develop and integrate CND/A Programs	P		Supported by SPJ60		
Develop CND concepts for Long Range Plan	P	S	S	S	S
Integrate CND/A into OPLANS/CONPLANS	S	S		Support to SPJ39	
Develop and advocate CND requirements in support of the JROC, JWCA, and IPL process.	P		S		
Review and develop requirements (MNS, ORD, etc.)	P		S		
Develop partnerships with Govt agencies, Civilian, Commercial, Coalition	S		Support to SPJ39		
J5 operational support to J29/39/69	P	S	S	S	S
CND/A conduit for J5	P				

Table D-5. J5 Tasks

5.1 CND/A Strategy Branch (SP/J59). The SP/J59 Strategy Division will ensure plans, policy and doctrine exist for CND mission execution. SP/J59 will provide integrated CND/A support to the Plans Directorate (SP/J5) and tailored CND/A support for other staff directorates. SP/J59 is the SP/J5 Directorate focal point for CND/A and will consist of two branches with specific orientation on CND and CNA activities, but an overall division focus on providing integrated IO/IW for the command. The SP/J59 mission is to plan, coordinate, review, assess, and program in support of the command's CND/A mission accomplishment. The J59 Strategy Division realizes that the missions of CND and CNA are interrelated and must be integrated into all plans, policies and doctrine; however, tasks associated with the CNA mission will be addressed in the CNA CONOPS at a later date.

5.1.1 Initial Focus. In accordance with its mission statement to ensure plans, policy and doctrine exist for CND mission execution, and within the constraints of resource allocations, the J59 will concentrate on the following areas:

5.1.1.1 Develop CND coordination internal (J2/3/5/6) to USSPACECOM.

5.1.1.2 Review USSPACECOM CONOPS and address CND operational impediments.

5.1.1.3 Define command relationships within DOD across the spectrum of conflict.

5.1.1.4 Leverage the USSPACECOM/DARPA/SPAWAR Information Operations Technology Symposium to build partnerships to assist the command mission execution

5.1.1.5 Review and assess policy impediments to CND exercises.

5.1.1.6 Support integration of CND into specific existing plans and requirements documents.

5.1.1.7 Advocate and support the establishment of a Colorado Springs Information Technology Center of Excellence for training and education (military, government, industry and academia).

5.1.2. Tasks Descriptions.

5.1.2.1. Facilitate and advocate CND Policy, Doctrine, and Legislation

a. Recommend, advocate, and coordinate policy, doctrine, and legislation for DoD network infrastructure defense on behalf of all DoD C/S/As to the Joint Staff. Specific areas of emphasis may include:

1. Policy, doctrine, and legislation that reflects the growing importance for the incorporation of information protection into all aspects of DoD mission operations.
2. Guidance for conducting CND in various operational environments, e.g., geographical areas, host nations, etc.
3. Guidelines for interacting with non-DoD and non-governmental agencies.

5.1.2.2. Integrate CND into War Gaming activities

a. Develop and disseminate tailored evaluations and lessons learned from Joint and Service IO/IW seminars, wargames and exercises.

b. Develop future concepts demonstrating CND capabilities with Joint and Service wargames within a variety of wargame scenarios.

c. Advocate for Joint and Service wargaming opportunities demonstrating CND strategies and capabilities. Work with wargame planners incorporating inputs to scenarios of future wargames.

d. As required, participate or observe wargames, and identify where strategies, TTP, or training and education concepts require further development in the realm of CND.

e. Provide feedback from wargame results to members of the USSPACECOM staff, so lessons learned can be incorporated into specific functional areas supporting the CND mission.

5.1.2.3. Develop and integrate CND/A Programs

- a. Develop and coordinate inputs for the Program Objective Memorandum (POM).
- b. Act as the point of contact and advocate for program issues concerning CND.

5.1.2.4. Develop CND concepts for the Long Range Plan

- a. Explore and develop concepts for the integration of CND strategy and capabilities into USCINCSpace's Long Range Plan. The concepts will provide a vision for information protection requirements for future war-fighters, and CND technologies which will evolve to meet the war-fighters' information protection requirements of the future.
- b. Develop concepts for the integration of CND strategy and resources into USCINCSpace's LRP. The concepts will provide a vision for how CND technologies will evolve to meet the war-fighter information protection requirements of the future.

5.1.2.5. Support integration of CND/A into OPLANS/CONPLANS

- a. Provide a framework, similar to OPLAN 3500-99 (Space Operations in Support of Regional Contingencies) that supports CINCs in the development of CND annexes to their specific OPLANS, and enhances indication and warning capabilities for effective CND.
- b. Ensure USSPACECOM deliberate planning focuses on inter-theater protection of the DII in order to support the execution of supported CINCs' OPLANS.
- c. Ensure USSPACECOM OPLANS/CONPLANS and supporting plans describe potential avenues and methods of attack an adversary could use against the DII.
- d. Provide an understanding of CND interdependencies among the CINCs, Services, and Agencies.

5.1.2.6. Develop and advocate CND requirements supporting the JROC, JWCA, and IPL process.

- a. Coordinate the IO Mission Area Working Group (MAWG).
- b. In coordination with J39, formulate and develop a DOD C/S/A CND capability overview and assessment for the JWCA community. Provide JWCA feedback on behalf of the C/S/As for new requirements for both resources and policy.
- c. Serve as the focal point to collect, integrate, and communicate USSPACECOM, JTF CND, and DoD C/S/A CND mission requirements and submit them into the joint-level requirements process.
- d. 1. Sources for requirements will often arise out of: regular interactions with DoD CND C/S/A "customers", particularly via the Space LNOs; after-action assessments of real world responses to intrusion/attacks; Joint Universal Lessons Learned from

exercise participation; vulnerability assessments; and, technological developments in network attack, intrusion detection, and attack response capabilities.

5.1.2.7. Review and develop requirements.

a. Advocate, develop and coordinate Mission Need Statements (MNS), Operational Requirements Documents (ORD), and Capstone Requirements Documents (CRD).

5.1.2.8. Develop partnerships with academia, government agencies, civilian, commercial, and coalition partners.

a. Advocate and support the establishment of a Colorado Springs Information Technology Center of Excellence for training and education (military, government, industry and academia).

b. Support partnerships with Government agencies and industry that contribute to a fully integrated defense-in-depth concept for the DII and NII.

c. Provide an open forum for all CND mission partners to provide input on changes required to policy, advances in technology, etc., to ensure defense-in-depth of the DII and NII.

d. Support the development of MOAs/MOUUs to define the cooperative interfaces between USSPACECOM and non-DoD government agencies and industry.

e. Build and sustain operational relationships with USCINCSpace mission partners. Ensure effective mutual support during crisis operations.

f. Attend conferences on information assurance-related activities and technologies hosted by other government agencies. As opportunities allow, present training, challenges and requirements to the DoD CND community.

5.1.2.9. J5 operational support to J29/39/69.

a. Support and participate in IO/IW/IA and technology-related conferences and symposiums.

b. Share concepts and technologies for conducting CND intelligence (J29) operations.

c. Define command relationships within DOD across the spectrum of conflict (J39).

d. Assess the integrated DOD/DII approaches and standard processes/ROEs for CND mission execution (J39).

e. Develop integrated strategies and provide for an interchange forum for all mission partners to provide feedback on advances required in policy, technology, etc.,

to provide in-depth defense of the DII (J39).

- f. Host conferences on CND for DOD C/S/As and all mission partners.
- g. Promote standardized CND training certification through the development of an Education Center of Excellence with academia for CND education and training, career development and professional growth.
- h. Share concepts and technologies for conducting CND command and control systems operations (J69).
 - i. Provide the interface between the J5 staff and the N-SP/J6 staff and CND-JTF/J6 in conducting and supporting CND command and control systems operations.

5.1.3. CND/A conduit for J5

- a. Provide the interface between the J5 staff and the J36, J39 and JTF CND staffs on operational support issues.
- b. Include in the conference schedule a segment to include an opportunity for interchange between DoD and non-DOD agencies, the private sector, academia, and if possible, foreign allies and coalition partners.
- c. JTF-CND. Conduit to J5 staff for JTF-CND Director for Plans, Policy and Exercises (JTF-CND/J5/J7) support.
 - 1. Provide the interface between the J5 staff and the JTF-CND J5/J7 responsible for planning contingency response scenarios, developing the TTP to support normal operations, and developing the plans to assure that CND procedures are synchronized with major military operations.
 - 2. Assist the JTF-CND J5/J7 in the development and integration of functional supporting plans into a coordinated defensive effort.
- d. Supported CINCs. Conduit to J5 staff for CINC coordination for CND Plans, Policies, Doctrine and Strategies associated with the defense of DOD computer networks impacting their area of responsibility (AOR) or mission capabilities.
- e. Components. Conduit to J5 staff for Service components for CND Plans, Policies, Doctrine and Strategies associated with the defense of DOD computer networks impacting their area of responsibility (AOR) or mission capabilities.

6.0. Directorate of Command Control Systems (J6). J6 will support the DOD CND mission with 14 of 32 manpower billets validated by the Joint Staff in September 1999. Until the validated manpower is on board, one officer and available contractor support will support J39C in the CINCs five priority CND tasks s described in paragraph 2.7.2.1 of the main CONOPS.

Provide SP/J39 technical support to develop, advocate, and maintain a comprehensive DII protection and planning framework that can be tailored to a specific C/S/A's mission or operations, to provide for standardized protection requirements and procedures for the DII	P	
Identify and maintain a technical model of the DII to map, visualize, and prioritize the components comprising the DOD network of computer systems to ensure network security is maintained and considered during the planning and design phases	P	
Act as technical advisor in the creation of protective measures and standards, technical and readiness standards, policy, doctrine and operational procedures	P	
Draft implementation recommendations and guide the DOD's use of certain technologies	P	
Formalize CND education, training, and awareness standards and requirements for users, operators, and other CND support staff	S	P = J37
Coordinate with defense and national level authorities, i.e., Defense-wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP), to ensure DOD CND efforts are in compliance with wider Information Assurance (IA) Critical Infrastructure Protection (CIP) policy and initiatives	S	P = J39
Support the JTF-CND and DISA to Operationalize and normalize execution of the CND mission. Standardize technical and operational incident reporting; integrate Service capabilities	S	P = J39
Develop partnerships and relationships with non-DOD agencies, private sector, and foreign allies/coalition partners for integrating responses to CNA	S	P = J39
Serve as technical advisor to accelerate system and network restoration through development of pre-planned preventive measures, such as back-up plans and/or architectures, attack-specific reactive tools or applications, or models and simulations.	P	
Support deliberate and crisis action planning	S	P = J39
Help develop CONOPS to integrate CND capabilities into policies, operations, plans, exercises, and training	S	P = J39
Coordinate technical assistance visits to C/S/A	P	
Work closely with J3 and J5 activities to translate operational requirements for automated CND tools into technical requirements. Advocate automated system requirements to appropriate C/S/A for development. Work with J3 to advocate CND automated systems for funding and	P	S=J39

implementation.		
Assist in establishing CND Standing Rules of Engagement	S	P = J39
Integrate, evaluate and assist in the deconfliction of DOD CND actions	S	P = J39
Advocate CND efforts in the evolution of the Global Information Grid	P	
Provide operational communication and computer support to J39:	P	
- See J39 tasks		
- Determine detectable events and methods		
- Long term trend analysis		

Table D-4. J6 Tasks

6.1. Mission. J6 serves as the technical CND subject-matter experts on the USCINCSpace staff; helps develop and advocate DoD standards for education, training, awareness, reporting technical analysis, etc. Develops and advocates , in coordination with DISA, integrated DII protection and planning framework; helps ensure CND requirements are reflected in plans, requirements documents, and COAs; and, supports partnerships and relationships with DoD and non-DoD agencies, allies, industry and academia.

6.1 .1. Task Descriptions

6.1 .1.1. Provide SP/J39 technical support to develop, advocate, and maintain a comprehensive DII protection and planning framework that can be tailored to a specific C/S/A's mission or operations, to provide for standardized protection requirements and procedures for the DII.

6.1 .1.2. Monitor the configuration management process for DOD systems and networks.

6.1 .1.3. Advocate changes to responsible agencies/groups to enhance defensive capabilities.

a. Solicit recommendations from C/S/As on how to improve CND operations and support to the DOD community.

b. Provide the technical voice for USSPACECOM, the JTF CND, and C/S/As on CND issues to any forums with involvement in establishing/changing matters such as policy, doctrine, legislation, technical capability requirements, operational procedures, etc.

c. Advocate CND requirements and issues to forums at the national level, including the Joint Staff, the IC, the NIPC, law enforcement, and other national agencies.

6.1 .1.4. Advocate and enforce the current Information Assurance Vulnerability Assessment (IAVA) process

6.1.1.5. Identify and maintain a technical model of the DII to map, visualize, and prioritize the components comprising the DOD network of computer systems to ensure network security is maintained and considered during the planning and design phases.

a. Using the DII network model, define the standard equipment and processes that are required to support CND for specific segments of the network. This model would then provide a reference to C/S/As to use in applying the standards required to maintain/upgrade their individual portions of the DII. For example, the model would define the standard monitoring and intrusion detection equipment, as well as system administrative practices that should be associated with particular segments of the network, such as a LAN or WAN.

6.1 .1.6. Act as technical advisor in the creation of protective measures and standards, technical and readiness standards, policy, doctrine and operational procedures.

a. Oversee the development of DOD technical directives and standards for DII CND operations.

b. Assist J39/J36 in developing SROE, Uls, CONOPS, TTP, etc. to provide guidance and direction for the conduct of CND operations.

c. Maintain currency on technical developments in CND and coordinate with the JTF CND and C/S/As to evaluate their applicability to CND operations (and implement if necessary).

d. Assist J59 in developing and advocating policy, doctrine, and legislation for DOD network infrastructure defense on behalf of all DOD C/S/As.

e. Assist J59 in developing and advocating technical and operational requirements for DOD CND operations on behalf of all DOD C/S/As.

6.1 .1.7. Draft implementation recommendations and guide the DOD's use of certain technologies.

a. Maintain currency on technical developments in CND.

b. Continually monitor and evaluate general CND threats and specific I&W to determine whether or not the implementation of specific technologies to counter the threat is warranted.

c. Provide recommendations for USCINCSpace approval directing the implementation of certain technologies/capabilities, based on threat analysis and the existence of technological capabilities to counteract the threat.

d. Support the Incorporation of promising emerging broad area technologies into USSPACECOM visions and plans for future operations.

6.1 .1.8. Formalize CND education, training, and awareness standards and requirements for users, operators, and other CND support staff.

a. Advocate standardized Joint training and certification requirements.

b. Establish a process and criteria for recommending minimum DOD training and certification requirements required to conduct advanced protection, monitoring, detection, response, and restore activities for CND mission operations.

c. Advocate CND operational awareness and technical training requirements to service schoolhouses and other DOD training activities/courses where possible (i.e. within DOD agencies).

d. Advocate CND operational awareness and technical training requirements to non-DOD government organizations, industry, and academia. Coordinate with these organizations developing common training and certification requirements.

6.1 .1.9. Coordinate with defense and national level authorities, i.e., Defense-wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP), to ensure DOD CND efforts are in compliance with wider Information Assurance (IA) Critical Infrastructure Protection (CIP) policy and initiatives.

a. Oversee JTF CND/GNOSC in assembling reports from C/S/As regarding DIAP and CAAP status and compliance to national IA and CIP initiatives.

b. Provide compliance status reports as required. Provide strategy and schedule for gaining adherence to required policy and directives as required.

c. Track the efforts of C/S/As to attain compliance to DIAP and CAAP IA criteria. Assist and coordinate technical support to their efforts if requested. Provide an interface between C/S/As and national-level IA representatives if required to coordinate compliance efforts.

6.1 .1.10. Support the JTF-CND and DISA to Operationalize and normalize execution of the CND mission. Standardize technical and operational incident reporting; integrate Service capabilities.

a. Assist J36/J39 in developing a normalized process for executing the CND mission by representing technical issues associated with CND operations. J6O involvement will include activities such as:

1. Participation in advocacy for policy and doctrine development.

2. Development of standards for CND hardware/software, administrative practices, technical terminology, and education and certification.

3. Assist in the development of intrusion detection, reporting, and restore processes across the spectrum of DOD networks and users.
 4. Participate in developing cooperative relationships with non-DOD agencies, industry, academia, and allied and coalition forces to establish and share warning/advisory information and technological solutions supporting CND.
 5. Integrate Service capabilities with other CINC and agency support to provide a broad base of operations and operations support to the DOD CND mission.
- 6.1 .1. 11. Develop partnerships and relationships with non-DOD agencies, private sector, and foreign allies/coalition partners for integrating responses to CNA.
 - a. Develop interactive partnerships with Government agencies and industry that will advance concepts and technologies in order to provide a fully integrated defense-in-depth of the DII and NII.
 - b. Assist in developing MOAs/MOUUs to define the cooperative interfaces and support capabilities between USSPACECOM and non-DOD government agencies and industry.
 - c. Normalize operations with mission partners so that efficient support can be mutually provided during crisis operations. This is important since portions of the DII ride on commercial networks.
 - d. Within the bounds of security requirements, share advisories and warnings of potential or actual intrusions, as well as analysis on intrusion characteristics, the selected restore plan, and lessons learned from responses to specific threats.
 - e. Share TTP, support tools, and lessons learned from vulnerability assessments, exercises, and real world activities.
- 6.1.1.12. Serve as technical advisor to accelerate system and network restoration through development of pre-planned preventive measures, such as back-up plans and/or architectures, attack-specific reactive tools or applications, or models and simulations.
 - a Formulate / advocate requirements for tools and applications to conduct CND activities, including monitoring and restoring computer networks.
 - b. Support S/PAN in fostering the development of analytical and network management tools that can guide development of defensive measures and prioritization of Physical and virtual network elements.
 - c. Coordinate with SN/SPAN in formulating/advocating requirements for modeling and simulation capabilities to perform development of COAs, validate TTP, conduct exercises and training, and perform timely, high-fidelity analysis of real world CNA threats.

6.1.1.13. Support deliberate and crisis action planning.

- a. Perform supporting CINC functions associated with both deliberate planning and crisis action planning activities.
 - 1. For deliberate planning, support the development and review of CINC OPLANS/CONPLANS for CND responses to various CNA threat scenarios.
 - 2. In crisis action planning, provide technical review and recommendation of COA options supporting specific CND objectives for a supported CINC.
- b. Provide assistance to the JTF CND or the affected C/S/As on the implementation of COAs/restore plans as required.
- c. In support of crisis operations, assist the SPOC, J39, and JTF CND in reviewing and selecting pre-existing restore plans/COAs. Selection criteria could include:
 - 1. The impact that implementation of the COA will have to current and planned mission operations.
 - 2. Resource and time requirements/availability to implement a restore action/COA
 - 3. The weighting of the impact between responding with a restore plan/COA vs. allowing an attack to continue in order to gather intelligence or evidence for prosecution.
 - 4. Depending on the restore plan/COA selected, assist in the modification of existing TTP, if required
- d. Provide technical inputs to any after-action review of COA, TTP effectiveness, and technical capabilities that may indicate where changes are required to more effectively combat a future CNA threat.

6.1.1.14. Help develop CONOPS to integrate CND capabilities into policies, operations, plans, exercises, and training.

- a. Provide technical inputs to CND CONOPS to ensure that CND concepts realistically reflect operational capabilities and interfaces.
- b. Assist in the integration of CND concepts into exercises and training activities and scenarios, as well as into daily operations and planning support activities

6.1.1.15. Coordinate technical assistance visits to C/S/A.

- a. Upon request from C/S/A, coordinate technical assistance visits to support a variety of activities, including the installation of network defense equipment, vulnerability assessments, education and training, and interpretation of CND policy and directives.

- b. J6O may coordinate resources for technical assistance from within the HQ USSPACECOM staff (or support contractors), or from other DOD and non-DOD agencies, and even academic support cells, if operations security permits.
 - c. As/if directed, schedule and coordinate no-notice staff assistance visits to determine C/S/A readiness to execute CND directives, and to assess the vulnerabilities of networks that are part of the DII.
 - d. Coordinate the NSA and DISA on red team scheduled activities to compile lessons learned for the entire DoD CND community.
- 6.1 .1. 16. Work closely with J3 and J5 activities to translate operational requirements for automated CND tools into technical requirements, Advocate automated system requirements to appropriate C/S/A for development. Work with J3 to advocate CND automated systems for funding and implementation.
- a. Provide expertise to develop a robust and flexible C2 technical architecture to enhance CND mission operations. The architecture should be able to accommodate advancements in CND technologies, changes in organizational structure, and, modifications to CND related policy and doctrine.
 - b. The C2 structure should provide for planning and execution of all USSPACECOM mission areas (CND, space, and future CNA), including automated tools to provide a capability to quickly obtain and maintain a situational awareness of DII network configurations, status, and CND mission planning and execution activities.
 - c. The C2 requirements should include capabilities for C/S/As to inter-operate with the JTF CND and USSPACECOM to conduct the DOD CND mission.
- 6.1 .1. 17. Assist in establishing CND Standing Rules of Engagement (SROE).
- a. Assist in the development of standing guidance under which all CND actors will operate and define activities for CND operations,
 1. Standing ROE must be specific enough to provide detailed guidance for anticipated CND activities. The guidance must consider the scope of authority and roles and responsibilities of all associated organizations. However, developers of the standing guidance must also be prepared to modify operational guidance, if required, to provide tailored direction as a potential CNA situation develops. This will be particularly true with respect to technical challenges and issues that are likely to unfold during a developing CNA scenario.
 - b. Closely coordinate products (perhaps even jointly develop) with the JTF CND to ensure technical and operational accuracy.
 - c. Assist J39 in developing and implementing thresholds or “trigger points” that require the JTF CND/SPOC to take immediate CND actions,

d. USSPACECOM-generated guidance will likely require frequent adjustments, since the process for responding to CNA within the DOD is fairly immature, as are support relationships and technologies for responding to CNA.

6.1 .1.18. Integrate, evaluate and assist in the deconfliction of DOD CND actions.

a. Maintain situational awareness of ongoing defensive and offensive DOD network operations.

1. A comprehensive offensive/defensive situational awareness may only be available at higher security levels than are conducted within SPOC operations. If so, deconfliction will be the responsibility of appropriately cleared personnel within J36 and/or J39.

b. Deconflict defensive and offensive planning activities so offensive operations do not nullify an ongoing or planned defensive operation.

c. Evaluate the situation and determine whether creating an integrated activity could potentially negate CND activities.

6.1.1.19. Advocate CND efforts in the evolution of the Global Information Grid.

a. Provide a DOD voice for the development of computer network defense-related technologies and capabilities as part of efforts to provide a truly global network within the DII (and potentially the NII). Present operational and technical requirements for conducting CND that are unique to DOD operations, such as the spectrum of operations and threats that DOD systems must be able to operate within.

6.1 .1.20. Operational communications and computer support to J39:

a. See J39 tasks (par 3.4).

b. Determine detectable events and methods.

1. Support J36, J39, and the JTF CND, establish and refine thresholds for identifying and categorizing CND events.

2. Work with J36, J39, and the JTF CND to establish and refine the operational reporting process, including thresholds that identify when up-channel reporting is required, and the type of information that is required during each level within the reporting process.

c. Long term trend analysis.

1. Collect data in the format similar to that collected for JMRR, DIAP, and CAAP reports and develop trend analyses for TBD time periods (monthly, quarterly, annually, etc.).

2. With OPSEC constraints, share trend analysis data with CND-related agencies and organizations external to the DOD, particularly the NIPC. Compare analyses to determine if there are trends in, for example, specific geographical areas, or against organizations supporting particular mission areas.

3. Apply results of trend analyses to address particular issues requiring emphasis, such as additional training for administrators/users, refinement of CND TTP, UIs, etc., or even requirements for technological developments to address specific network vulnerabilities.

d. Provide a support interface between the J6 staff and the daily operational activities of the SPOC/J36/J39 and the JTF CND.

1. Reachback to additional J6 resources when required for tasks such analysis of intrusion advisories/warnings, assessing the potential for collateral impacts if a suspected intrusion migrates to other networks, and the development/selection of COAs in response to a CNA threat.

7.0. Staff Judge Advocate (SJA)

7.1. Mission Statement. AFSPC/JA will advise USCINCSpace and his staff on the legal implications of developing, promulgating, and executing doctrine in furtherance of the CND mission

7.1 .1. Task Descriptions

7.1 .1.1. Work with the staff to develop doctrinal options for accomplishing the CND mission that comply with the law.

7.1 .1.2. Ensure that the command's interests are properly advocated to the individuals and organizations that can shape the development of the law in this area.

7.1 .1.3. Provide guidance to the JTF-CND/JA on issues of law and policy that affect the conduct of CND operations.

7.1 .1.4. Educate the USSPACECOM staff on the existing legal limitations affecting CND operations.

7.1 .1.5. Assist in the negotiation, or other development, as appropriate, of agreements or memoranda that permit the conduct of CND operations in furtherance of the USSPACECOM mission that might implicate the sovereign interests of other nations

8.0. Public Affairs (PA)

8.1. Mission Statement. PA develops public affairs communication strategies, public affairs guidance (PAG), products (releases, web pages, fact sheets, etc.) to promote and support the CND mission for USCINCSpace.

8.1.1. Task Descriptions

8.1 .1.2. Schedule and coordinate media (internal/external) interviews and events with USSPACECOM senior leaders.

8.1 .1.3. Schedule, coordinate media (internal/external) interviews and events with CND subject area experts.

8.1.1.4. Prepare and distribute timely news advisories and releases for internal/external media.

8.1 .1.5. Prepare wide-variety of CND products (e.g. web pages, key command messages, fact sheets, etc.) for the USSPACECOM public web site and SIPRNET.

8.1 .1.6. Prepare and distribute Public Affairs Guidance (PAG) which includes general guidance and specific Responses to Queries (i.e. Questions and Answers).

8.1 .1.7. Coordinate PA exercise participation with SPJ37, J5 , and other directorates and agencies as. required.

8.1 .1.8. Coordinate PA strategies with component commands and counterparts at other government agencies.

8.1 .1.9. Provide input/manning to Special Technical Operations (STO) as required.

8.1 .1.10. Constantly evaluate plans, procedures, and processes to improve public affairs support to the CND mission.

Task	JA	PA	Comments
Develop key CND communication messages		P	
Schedule and coordinate media events		P	
Prepare and distribute news releases		P	
Prepare products for public web sites		P	
Prepare and distribute PA guidance		P	
Coordinate PA exercise participation		P	
Coordinate PA with components/C/S/As		P	
Support STO as required		P	
Update PA portion of Plans		P	
Develop legal CND doctrinal options	P		
Shape CND law in Command's interest	P		
Provide CND legal guidance to JTF-CND	P		

Educate USSPACECOM staff on CND law	P		
Assist in negotiation with CND partners	P		

Table D-5. Other CINC's Staff Tasks

UNCLASSIFIED

HEADQUARTERS, U.S. SPACE COMMAND
250 S Peterson Blvd, Suite 116

Peterson AFB, CO 80914-3010
01 October 1999

USSPACECOM Computer Network Defense (CND) Concept of Operations (CONOPS)

ANNEX 2 US SPACE COMMAND CND CONOPS

Table Of Contents

List of Figures	
Fig I-I. The Interactive Nature of The CND Mission	4
Introduction.	1
Purpose	1
Threat	2
Concept of Intelligence Operations	3
Duties and Responsibilities	4
Production Activities	8
Resources	9

REFERENCES:

- a. Joint Strategy Review (draft), 28 July 99 (SNF)
- b. National Intelligence Estimate (NIE) 97-9/I, classified title, vol. 1, July 1997 (SNF).
- c. USSPACECOM/J2 Global Information Operations Threat Briefing, 11 May, 1999 (SNF);
- d. JTF-CND/J2 Tactics, Techniques, and Procedures (draft), (SNF)

1 .0. INTRODUCTION

1 .1. Purpose

1.1 .1. This annex sets forth the command relationships and responsibilities of USSPACECOMN2, Intelligence Directorate, in the execution of the Computer Network Defense (CND) mission. It contains goals and objectives for assuming the mission as military lead for CND and provides overarching guidance to the HQ USSPACECOM staff for employing intelligence support in executing the mission.

1 .1.2. The role of USSPACECOMN2 is to ensure that USCINCSpace has the

UNCLASSIFIED

intelligence necessary to discharge the assigned CND mission, with emphasis on operational decision making at JTF-CND and at HQ USSPACECOM through the Space Operations Center (SPOC), or at the Mobile Consolidated Command Center (MCCC) when deployed.

1.1.3. It is the goal of USSPACECOMN2 to become the center of excellence for indication and warning of threats to computer networks and the vital information that flows through them. Timely, all-source intelligence is the key to determining adversarial intentions and in activating the warning indicators that tie strategies to real time events enabling rapid decision making. Effective intelligence support to CND is both critical and demanding due to its urgency, scope, and complexity. Intelligence must support the entire spectrum of joint (and, when required, combined) operations to help ensure the greatest possible security for DoD information, computers, and networks.

1.1.4. The objective of USSPACECOM J2 is to enhance the synergy between mission partners, thereby pulling together all intelligence community resources to satisfy CND intelligence requirements. Fused intelligence, from multiple sources, will provide the clearest and most reliable picture of the cyber battlespace. Additional information will be provided in Appendix 5, Intelligence Community Partners,

2.0. **Threat.** The ability to attack or influence information infrastructure, particularly computer networks, is a growing and complex threat to national security. Within the realm of Computer Network Attack (CNA), technology and expertise is readily available on a worldwide basis both in and outside of governments. The problem is exacerbated by the fact that CNA can, and does, take many forms. CNA manifests itself as a discipline within established strategy and doctrine; a terrorist weapon aimed at a specific, localized target; a hacker tool designed to invade, influence, destroy or manipulate data; a strategic weapon meant to create confusion, distrust, and disruption as part of a larger attack. It is conducted by nations, groups, and individuals. Attacks are coordinated and well planned; they are the work of a small, non-cohesive group that comes together for the purpose of a single operation then disbands; attacks are conducted by a single, highly trained computer expert who is working alone or acting as a cyber mercenary. CNA originates from a military facility; a basement; a pay phone; a university. The reason for an attack is national interest; personal motivation; ethnic, cultural, religious, and political difference; financial gain; and military strategy. A computer network can be penetrated and weapons left to "detonate" at a designated time well in the future, effectively eliminating the possibility of attribution. CNA is not a single discipline and cannot be defended as if it were. It is one of the most complex and challenging threats that the Intelligence Community has ever faced.

2.1 The U.S. DoD has made a significant investment in information technologies and is dependent upon its use. Many potential enemies see the U.S. dependence on its technologies as an Achilles heel that can be effectively exploited. In addition, most U.S. military networks are not isolated, but rather are a part of a larger, global

UNCLASSIFIED

commercial infrastructure. As a result, the U.S. is probably the most vulnerable nation in the world to CNA. More and more countries, groups, and individuals are recognizing the potential damage that could be done to the U.S. and as a result, the threat is growing in both scope and complexity. A number of nations, having recognized the potential of CNA as a major force multiplier, are incorporating it into their formal strategy and doctrine and developing weapons, tactics, and procedures for its use. CNA doctrine includes traditional military targets such as C3 nodes, and less traditional ones such as national banking and financial infrastructures. Unlike other military disciplines, CNA capability is not limited by force size or budgets. Instead, it is limited only by expertise and imagination, and can be conducted by nation states, trans-national groups, or individuals.

2.1.1. See References a – c for latest information concerning threats posed by specific countries.

3.0. Concept of Intelligence Operations. US Space Command Intelligence will utilize all sources and facilities in the Combined Intelligence Watch (CIW), the Combined Intelligence Center (CIC), the JTF-CND, and partnerships with C/S/As to provide timely I&W, assessments, estimates, and predictive analysis products supporting the protection of friendly computer network infrastructure and information.

3.1. JTF-CND/J2 is responsible for all aspects of intelligence support to the Commander, staff, and components of JTF-CND. Intelligence support will be coordinated with USSPACECOMN2 to ensure unity of effort and will be conducted in accordance with ref d. JTF-CND/J2 may conduct direct liaison with any element of the intelligence community contributing to the CND mission.

3.1.1. USSPACECOMN2 has designated CJTF-CND as the lead consumer for operational intelligence support, which will be provided in accordance with Joint guidance. Specific responsibilities and division of labor for USSPACECOM/J2 and JTF-CND/J2 will be codified in a future USSPACECOM/J2 Tactics, Techniques, and Procedures (JTTP). This document will be coordinated with appropriate mission partners to ensure maximum synergy of intelligence resources.

3.2 Effective Tactical Warning and Attack Assessment requires overlapping efforts from the J2/J3/J6 communities. Additionally, the capabilities of C/S/As for information sharing, deconfliction and assessment are critical to successful CND efforts. J2FX will fuse available intelligence inputs and provide assessments as required to CND Watch Officers in the SPOC, who will integrate J2/J3/J6 inputs to assist operational decision making. The figure I-I below depicts this integration.

UNCLASSIFIED

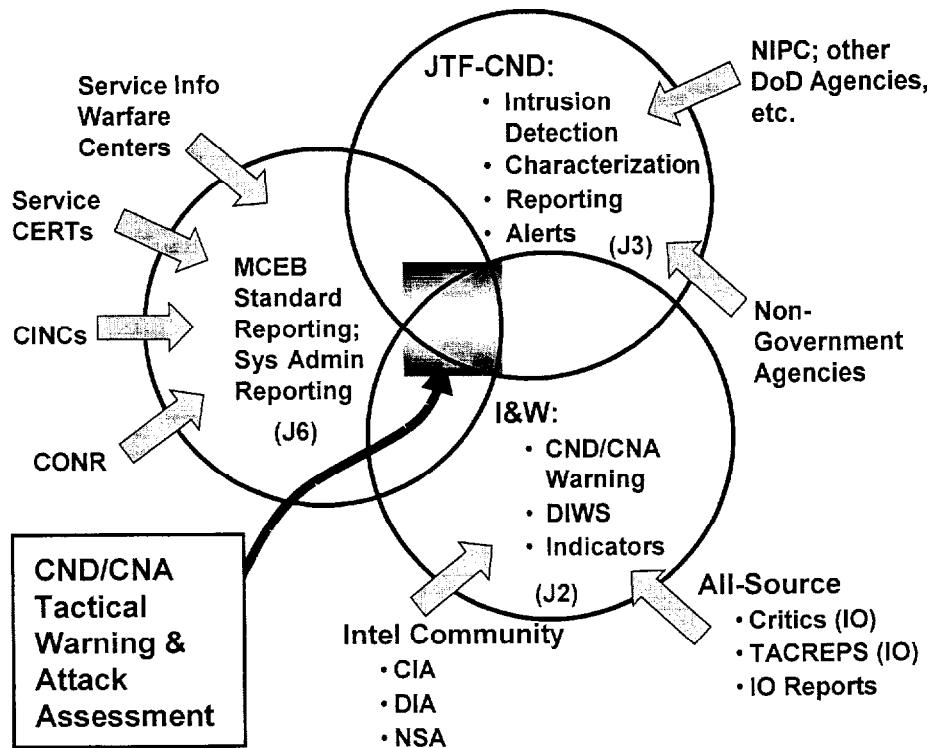


Figure I-I The Interactive Nature of the CND Mission

3.3.3 This CONOPS is a living document. As detailed processes and procedures evolve from working with our Mission Partners, particularly those concerning strategic (both long-term and global) responsibilities, the Intelligence Directorate will document those developments in this annex. Additionally, we will revise established procedures as required to effectively accomplish the mission, and document those revisions in this CONOPS in a timely manner.

4.0. USSPACECOM/J2 Duties and Responsibilities

4.1. General Tasks. USSPACECOMN2 will perform the following tasks in coordination with C/S/As as required:

4.1.1. Assist J3/J5/J6 in developing CINC Priority Intelligence Requirements to drive I&W, intelligence production, collection management, nodal analysis, and threat assessment efforts.

4.1.2. Develop relevant and timely Information Requirements (IRs) CND Collection Requirements (CRs), Request For Information (RFIs), and Production Requirements (PRs) processes.

4.1.3. Develop CND threat assessments and estimates as well as country studies in

UNCLASSIFIED

support of necessary intelligence production.

4.1.4. Conduct in-depth analysis of long term indicators in support of global CND-shaping strategies.

4.1.5. Develop an effective integrated information fusion capability with other information-sharing providers like system administrators, counter-intelligence, and law enforcement agencies.

4.1.6. Integrate CND intelligence scenarios into exercises and wargames

4.1.7. In coordination with J3 and J6, establish an effective 24 x 7 CND threat warning and attack assessment capability including reporting procedures, required core competencies and training standards.

4.1.8. In coordination with J3/J6 and Mission Partners, establish standardized CND event, incident, and intrusion reporting criteria and format. (Protect, Detect and Assess, Respond, and Restore)

4.1.9. Coordinate with DIA to integrate CND into WATCHCON and INFOCON criteria and processes.

4.1.10. Establish responsive CND threat analysis and operational intelligence capabilities through the Information Fusion Branch (J2FX).

4.1.11. Ensure analyst familiarity with, and access to, CND products and services.

4.1.12. Determine and submit requirements for resources to optimize intelligence supporting the DOD CND Mission.

4.1.13. In coordination with JAG, J3, J5 and Mission Partners, establish criteria and processes for fastest possible resolution of Intelligence Oversight Issues.

4.2. Specific Tasks. The USSPACECOMN2 will support Tactical Warning and Attack Assessment commencing 1 Oct 99. Due to resource constraints, intelligence support for the CND mission will be provided along functional lines across the entire directorate. As additional manning becomes available toward the end of FYOO and as processes and procedures are defined with Mission Partners, J2 will round out its support for strategic (longer-term and global) issues. Specifically:

4.2.1. J2F Combined Intelligence Center will:

4.2.1.1. Through J2FX and J2FZ, provide one qualified, on-call intelligence analyst

UNCLASSIFIED

(active duty, government service, or reserve component) to assist SPOC CND Watch Officers with appropriate intelligence assessment of attacks or intrusions on a 24-hour/day basis. Such support will be coordinated between J2FX/Z under the purview of the CIC Commander.

4.2.1.2. In conjunction with J2X, provide input to J3/5/6 concerning core analytical competencies for CND Watch Officers.

4.2.1.3. Through J2FX/C and in conjunction with J2X, assist J3/5/6 in developing CINC Priority Intelligence Requirements to drive Indications and Warning, intelligence production, collection management, nodal analysis and threat assessment efforts. (See Appendix 2.)

4.2.1.4. Through J2FC, provide collection management support as described in Appendix 1.

4.2.1.5. Through J2FX develop CND threat assessments and estimates as required, to eventually include country specific threat documents in support of the command mission.

4.2.1.6. Ensure appropriate collateral-level threat documents are posted and updated as necessary for users at the SECRET level via INTELINK.

4.2.1.7. In conjunction with J2S, develop procedures for transition of on-call analysts to CND Intelligence Watch in J2S once active duty assets become available.

4.2.1.8. When faced with technical questions concerning NIPRNET and/or SIPRNET, contact locally available (J6, AFSPACE SC, 721st or 21st Comm Squadron) experts on those networks or DISA as network owner.

4.2.1.9. J2FZ will support USSPACECOM J39 with two full-time intelligence personnel. Primary duties, as currently envisioned, are to coordinate reach-back to J2F through J2FX in support of CINC requirements for operations, Y2K, exercises, and policy.

4.2.2. J2S Strategic Warning and Readiness Division will:

4.2.2.1. Provide support to J-39 for COMMAND APOLLO and other CND exercises, as required.

4.2.2.2. In conjunction with J2X, provide J3/5/6 with recommendations concerning core intelligence competencies for CND Watch Officers.

4.2.2.3. Provide support in conjunction with J2F, through a 24/7 Intelligence Watch in

UNCLASSIFIED

J2S, to serve as primary J2 focal point for CND actions.

4.2.2.4. Maintain recall rosters for J2 personnel and initiate recall procedures IAW SOPS.

4.2.2.5. When faced with technical questions concerning NIPRNET and/or SIPRNET, contact locally available (J6, AFSPACE SC, 721st or 21st Comm Squadron) experts on those networks or DISA as network owner.

4.2.2.6. Participate in CND Threat Assessment/Attack Assessment.

4.2.3. J2X Intelligence Policy, Plans, and Programs Division will:

4.2.3.1. In conjunction with J2Z, convene a J2 CND Working Group to develop internal processes and resolve issues, as required.

4.2.3.2. In conjunction with J2Z, convene external working groups to develop processes and resolve issues with Mission Partners, as required. (See Appendices 5 – 7 for Strategic issues.)

4.2.3.3. Document developed processes and resolved issues in this Annex, as required.

4.2.3.4. In conjunction with J2F, arrange for Reserve Component support for CND duties, including deconfliction of duty schedules and attendance at required training.

4.2.3.5. Through J2XR and in conjunction with J2F, determine and document required training for CND Watch Officers in the J2 Master Training Plan.

4.2.3.6 Through J2XR, and in conjunction with J2F, develop and implement strategies for virtual tasking of Reserve assets, especially for analysis of OSINT.

4.2.3.7. Through J2XX, ensure appropriate CND inputs are included in planning documents.

4.2.3.8. Through J2XX, and in conjunction with Mission Partners, apply analysis of long-term indicators to recommend global-shaping CND strategies for the annual Joint Strategy Review and other strategy documents.

4.2.3.9. When faced with technical questions concerning NIPRNET and/or SIPRNET, contact locally available (J6, AFSPACE SC, 721st or 21st Comm Squadron) experts on those networks or DISA as network owner.

01 OCTOBER 1999

UNCLASSIFIED

UNCLASSIFIED

4.2.4. J2Y Intelligence Systems Division will:

4.2.4.1. Respond to requirements from the J2 analytical/collection community to develop, integrate, and maintain automated tools for tasks related to the CND mission such as modeling, threat database, and activity analysis. Maintain isolated test environment for CND product integration and problem resolution just as with any other software application.

4.2.4.2. Develop a J2 strategy for ensuring protection of SCI networks in conjunction with Mission Partners (see Appendix 5).

4.2.5 J2Z will:

4.2.5.1. Develop and coordinate the J2's transition plan to provide CND/A support to the CINC, staff, and components from Initial Operational Capability (IOC) to Full Operational Capability (FOC). This billet is temporary and will be eliminated not later than FOC of both missions.

4.2.6. J2AC Counter Intelligence will:

4.2.6.1. Provide support as described in Appendix 3, Counterintelligence.

4.2.7. FDO Foreign Disclosure Office will:

4.2.7.1. Provide support as described in Appendix 4, Foreign Disclosure.

4.2.8. All Divisions will:

4.2.8.1. Appoint a division representative to the CND Working Group and notify J2Z of this appointment.

4.2.8.2. Forward Annex updates to J2XX for inclusion in revised drafts for inter-division coordination.

5.0. INTELLIGENCE PRODUCTION ACTIVITIES.

5.1. Products. CND products will be developed by the Combined Intelligence Center Information Fusion Branch to support the Command's CND mission. Specific product listings will be included in future CONOPS revisions, Reserve Component assets will contribute to Intelligence Production whenever feasible, to include employment of Joint Intelligence Reserve Centers (JRICs).

UNCLASSIFIED

5.1 .1. Other Intelligence Products. Other estimative products will be produced as required. Products releasable to Canada will be developed and disseminated as practical.

5.1.2. Dissemination. Intelligence will be disseminated to command and worldwide consumers and updated as required by the Combined Intelligence Center. Products at the collateral level will be produced, posted, and updated on INTELINK whenever feasible. Products releasable to Canada will be disseminated as practical.

6.0. RESOURCES

6.1. No additional resources are expected to arrive until the end of FYOO. At that time, we expect only a small increment (4 persons). In-house support from across all divisions will be judiciously applied to provide support for the CND mission with the minimum impact on J2 support for the space mission.

6.1.1. J2 will provide two analysts to J-39 to assist command efforts for the following USCINCSpace-identified priorities: 1) Real-world operational support, 2) Y2K issues, 3) Exercises, 4) Policy Issues.

6.1.2. Representatives will coordinate closely with appropriate J2 divisions to resolve issues and compare taskings.

6.2. As active duty manning becomes available, the following functions will be accomplished by the J2 Divisions:

6.2.1. J2F Combined Intelligence Center

6.2.1.1. Civilian Positions, The global scope of these positions will require that they be filled at the mid-career level (GS-12/13). Due to the ever changing, highly technical, fast pace, near-real-time analytical responsibilities of these positions, the incumbents will require a high degree of experience and breadth of knowledge in a variety of disciplines, including Information Operations (IO). Because of the nature of the intelligence analysis in which they will be engaged, they must have a thorough grasp of the complexities of intelligence oversight requirements as well as have the flexibility to handle both traditional intelligence analysis and asymmetric threat assessment. These analysts will routinely be called upon to brief and advise high ranking officials within NORAD/USSPACECOM as well as other senior decision makers within the Intelligence Community and throughout the DoD and other government agencies and departments. Each of these individuals will have to define objectives, conduct independent analysis, interact with collection experts, and prepare finished reports on foreign IO. They will be expected to develop, propose, and implement new

UNCLASSIFIED

approaches to solving complex analytic problems, identify trends in foreign employment of IO capabilities, recognize adoption and implementation of IO doctrine, and understand the application of IO in asymmetrical threat environments. Incumbents in these positions will have to establish and maintain close working relationships with a broad spectrum of other analytic agencies and communities, including some that are highly technical in nature. They will have to carry out liaison efforts with other agencies both in and out of the DoD on a daily basis. All-source data will be fused with information derived from national level studies, estimates and projections. Many tasks will be performed in a near-real-time operational environment. Analysts in these positions can expect to travel on a regular basis and will be required to work hours outside of what is considered normal duty hours, including shift work.

6.2.1.2. Officer Positions. Under announced UCP changes, USSPACECOM will be responsible for defining, monitoring, coordinating, and reporting on worldwide Information Operations threats against DoD computer networks. Officers assigned to the Combined Intelligence Center will be responsible for identification, analysis, and reporting of these threats across the entire spectrum of conflict, including asymmetrical and non-traditional operations. They may also be involved in the development and implementation of DoD-wide guidelines for CND as well as liaison with non-DoD agencies for purposes of coordination. Some positions will be primarily responsible for supervision of the development and maintenance of threat scenarios, while others will be responsible for the proper development and application of Indications and Warnings methodologies to the IO problem. All of the personnel assigned can expect to prepare and present briefings and create products for senior decision makers at NORAD/USSPACECOM, within the Intelligence Community, and throughout the DoD and other government agencies and departments.

6.2.1.2. Enlisted Positions. Enlisted personnel will be expected to have the requisite level of technical expertise and analytic experience to deal with the complexities of the intelligence challenges inherent in the CND problem. Technically, they will be required to be able to understand and react to hostile attacks against DoD information systems under both traditional and asymmetrical conflict environments. Analytically, they must be able to demonstrate in-depth analytic, research, and reporting skills. Analytic reporting will encompass both long term assessments as well as near-real-time crisis reporting. Senior enlisted personnel can expect to regularly brief senior command decision makers on Information Operations and threats to DoD Information Systems. Certain personnel may be assigned to assist in the management of Indications and Warning System Warning Problems as well as overall warning indicator development. Analysts must either have or be able to develop a thorough understanding of the differences between Warning and Current Intelligence. Personnel will also be expected to have or be able to develop a solid working knowledge of computer systems, networks, and potential threats to information systems such as viruses, worms, time bombs, etc. All personnel assigned will develop and maintain strong working relationships with other analysts within the Intelligence Community and

UNCLASSIFIED

throughout the DoD.

6.2.1.4. Contractor Positions. J2F will require five additional personnel to provide specific technical analysis of various computer networks and the detailed understanding to trace potential attacks against DoD or command systems. This type of expertise currently does not exist in large numbers within the DoD system and additional resources would be required for successful mission accomplishment.

6.2.1.5. Collection Manager. The IO collection management officer (CMO) will be responsible for the development, processing, submission and tracking of the command's IO collection requirements to the Intelligence community. The IO CMOs will coordinate for National collection from all four primary sources of intelligence (IMINT, SIGINT, MASINT, and HUMINT) and will also be the principle advisor to the other unified commands on IO collection requirement issues and submissions.

6.2.2. J2X Intelligence Policy, Plans and Programs Division

6.2.2.1. Deputy/J2XX Branch Chief. Provides continuity for all J2 CND/A policy, strategy, and doctrine. Fluent in all aspects of computer issues/architectures and their effect on J2 planning. Primary interface for coordination/deconfliction of intelligence processes impacting on CND/A with National Agencies, the Joint Staff J2, and intelligence organizations in other commands. Works with JS staff and other headquarters planning activities to ensure J2 interests and requirements are thoroughly integrated into command-level packages. GS-13/14, 0334

6.2.2.2. CND/A Planner. Develops intelligence inputs for NORAD-USSPACECOM plans, Joint Publications and other planning documents for effective support to CND/A operations. Serves as Future Operations Branch planner in the Space Operations Center during contingencies. Deconflicts allied and coalition intelligence processes, architectures, and policy supporting CND/A operations. AF 0-3/4, 14N3.

6.2.2.3. CND/A Planner. Alternate Future Operations Branch Planner during contingencies. Reviews NORAD-USSPACECOM plans, Joint Publications, and other planning documents for discrepancies in intelligence processes which would hinder effective support to the CND/A mission. Deconflicts local intelligence processes required for effective CND/A support. Identifies Intelligence Oversight and related issues requiring resolution for effective intelligence support to CND/A operations. Prepares staff packages for coordination within NORAD-USSPACECOM on intelligence issues with legal, operational, or strategic CND/A implications. Prepares staff packages for internal coordination to resolve issues with impact on intelligence support to CND/A. USN E-7/8

6.2.2.4. CND/A Technical Doctrine Interface Analyst. (Two positions) Ensures intelligence processes, connectivity, and procedures are consistent with Joint Doctrine

UNCLASSIFIED

and Command policies. Identifies inconsistencies and recommends solutions for action by J2 planning staff. Provides technical expertise and inputs to J2 planning and architecture activities to ensure technological advances are continuously taken into account. (Contractors)

6.2.3. J2Y Intelligence Systems Division

6.2.3.1. System Administration Contractor. Is responsible for day-to-day administration of CND data analysis systems either internally developed or provided by external entities as community assets. Contractor system administrator for security tools. Several tools will be involved such as ESM, ITA, TIVOLI, and various firewalls and guards as well as macro-network level tools such as NETVIZ and follow-ons. Reports to NSPJ2YMS or designated representative.

6.2.3.2. Contract Software Developers (Two Positions). Develop and maintain site-specific applications to support J2 CND analysts. Requires in-depth knowledge of various programming languages and operating systems and some familiarity with computer security issues to include intrusion detection and reporting procedures. Reports to NSPJ2YMS or designated representative.

6.2.4. Reserve Component Manpower

6.2.4.1. J2 has identified eight Reservists within the Joint Aerospace Reserve Program (JARP) who are qualified and willing to assist J2FZ in assuming responsibility for on-call CND analysis beginning 1 Oct 99. In some cases, additional training may be desirable. J2XR is responsible for notifying these Individual Mobilization Augmentees of their selection for this duty and for coordinating with J2FZ concerning duty schedules, reporting chain, and training. J2XR will provide required support for JARP Reservists per standard procedures. J2F will be responsible for supervisory responsibilities of IMAs per standard procedures.

6.2.4.2. J2XR will, in conjunction with the CND Activation Task Force, identify and arrange for other Reserve Component intelligence augmentation consistent with the Command CONOPS.

//SIGNED//

P.S. LEWIS
CAPT USN
DIRECTOR OF INTELLIGENCE

HEADQUARTERS, U.S. SPACE COMMAND
250 S Peterson Blvd, Suite 116
Peterson AFB, CO 80914-3010
1 September 1999

USSPACECOM Computer Network Defense (CND) Concept of Operations (CONOPS)

Appendix A - Minimum Mission Resources

Minimum Resources to Activate USSPACECOM CND Mission. USCINCSpace established 22 positions as the minimum personnel required to activate the USSPACECOM CND mission on 1 Oct 99. Table 4-I lists the distribution of the 22 positions throughout the command and consists of 17 military (17 officer, 0 enlisted, 5 civilians) plus 5 contractor technical support.

Line #	Ofc Sym	Title	Service	Grade	Skill Code
01	SP/JA	Legal Officer	AF	O 5	51J4
02	SP/J2	Intel Officer	AF	O2/O3	14N3
03	SP/J2	Intel Officer	AF	O2/O3	14N3
04	SP/J2	Intel Operations Officer	AF	O2/O3	14N3
05	SP/J2	Intel Operations Officer	AF	O 4	14N4
06	SP/J39	Division Chief	AF	O 6	13S4
07	SP/J39C	Branch Chief	AF	O 5	13S4
08	SP/J39C	CND Operations Specialist	AF Civ	GS-12	13S4
09	SP/J39C	CND Operations Officer	AF	O 4	13S4
10	SP/J39I	CND Integration Manager	AF Civ	GS-12	13S4
11	SP/J39I	CND Integration AO	AF	O 4	13S4
12	SP/J36	Watch Officer	AF	O 4	13S4
13	SP/J36	CND Plans Officer	AF	O 4	13S4
14	SP/J36	LNO – ACOM	AF	O 5	13S4
15	SP/J36	LNO – Joint Staff, OSD	AF	O 6	13S4
16	SP/J37	CND Exercise Plans Spec	AF Civ	GS-12	13S4
17	SP/J59D	Requirements Development	AF	O 5	33S4
18	SP/J59D	Requirements Officer	AF Civ	GS-12	33S4
19	SP/J59D	Wargames/Exer/Strat Officer	AF	O 4	13S4
20	SP/J69X	Branch Chief	AF	O 5	33S4
21	SP/J69Y	Comm & Info Officer	AF	O 4	33S4
22	SP/J69C	Computer Specialist	AF Civ	GS-13	33S4

TABLE A-I. Minimum Position Distribution

Appendix B - REFERENCES

Unified Command Plan 1999

CJCSI 6510.01 B Change 1, 26 Aug 98, Defensive Information Operations

Joint Strategic Capabilities Plan

Joint Publication 2-0, "Joint Doctrine for Intelligence Support to Operations"

Joint Publication 3-I 3, "Joint Doctrine for Information Operations"

Joint Publication 5-0, "Doctrine for Planning Joint Operations"

USSPACECOM Computer Network Defense Implementation Plan

Appendix C

Key CND Terms, Phrases and Definitions

This appendix provides standard DoD terms, phrases and concepts related to computer network operations. These terms are commonly used throughout the CND I-Plan and CND CONOPS. They provide a common semantic framework to further understanding of the USCINCSpace CND mission. The terms and phrases below were extracted from Joint Pub 3-13 and CJCSI 6510.01 B, Change-I. As USSPACECOM and JTF-CND CND mission operations experience increases, CND terms and phrases may be adjusted.

- a. Computer Network Defense (**CND**). Measures taken to *protect and defend* information, computers, and networks from disruption, denial, degradation, or destruction (source: CJCSI 6510.01 B, CH-I, emphasis added).
- b. Event, Intrusion and Incident. (See the figure C-I below).
 1. Event. Activity on a computer system or network consisting of an known/observed action, e.g., printing, log on, etc., directed at a target, e.g., printer, server, etc. Reference Figure 3-I. Events may or may not be unauthorized or hostile in nature.
 2. Intrusion. A set of activities on a computer system or network consisting of a known/observed tool, e.g., program, data tap, etc., used to exploit a system/network vulnerability to execute an event which results in an unauthorized result, e.g., increased access, denial of service, etc. Reference Figure C-I. A series of related intrusions are referred to as an intrusion set
 3. Incident. A specifically known/observed or categorically described intruder, e.g., Nation State with a specific capability and doctrine, Ego-driven hacker, etc., executing a set of related intrusions into a computer system/network to achieve a desired objective, e.g., ego thrill, damage, CNE of information, etc. Reference Figure C-I.
- c. Attack. Per JP 3-1 3 for computer network attack, operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. For the purpose of this CONOPS, attack is a subset of intrusions.
- d. Odyssey Collaboration System. Prototype collaborative environment sponsored by USPACOM, being demonstrated to the JTF CND and USSPACECOM by DISA. The tool provides connectivity at the CINC level to appropriate C/S/As for the purpose of communication, coordination, planning, and directing the CND mission.

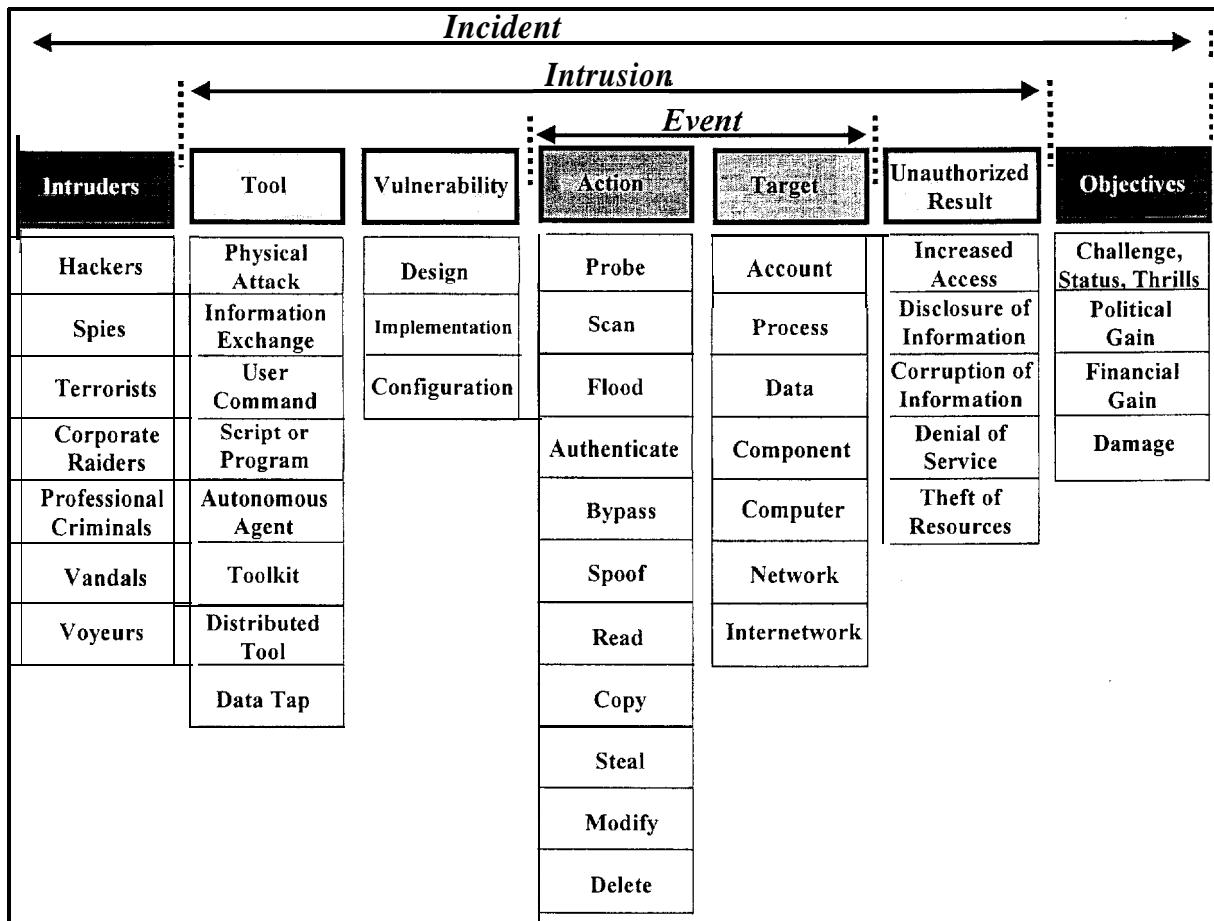


Figure C-I. CND Taxonomy

e. Combatant Command (COCOM). COCOM authority is defined by Title 10 ("Armed Forces"), United States Code, section 164, as: "Combatant Command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority)."

f. Coordinating Authority. Coordinating Authority is defined by Joint Publication (JP) I-02 as: "A commander or individual assigned responsibility for coordinating specific functions between two or more Military Departments or two or more forces of the same Service. The commander or individual has the authority to require consultation between

the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations."

g. Delegated Authority. On 1 Oct 99, USCINCSpace will delegate the authority to execute CND operations to the commander, JTF (CJTF) in support of the DoD. This includes all actions and responsibilities required for monitoring and evaluating security incidents in the DII, developing and coordinating response actions with all CINCs, Military Services, and agencies (C/S/A), and directing and executing response action that do not breach the established thresholds. This authority includes exercising tactical control (TACON) of assigned CND forces.

h. Directive CND Actions. The act of developing and executing response COAs to mitigate, block, or defeat intrusions in to the DII on behalf of the DoD. Presumes understanding of the implication and impacts to DoD operations and missions. Includes the provision for C/S/A reclama and notification to USCINCSpace should a C/S/A not be able to comply with the timing or specific actions directed.

i. Fragmentation Order (FRAGO). Abbreviated for m of an operations order usually issued on a day to day basis, that eliminates the need for restating information contained in the basic operations order. It may be issued in sections.

j. Future Operations Branch (FOB). SPOC operations, support, and planning staff. The FOB focuses on current operations out past 72 hours.

k. Headquarters Staff Actions, Actions taken by USSPACECOM staff up to the Directorate level flag officers, e.g., SPJ3, SPJ6, etc., and distinguished from action taken by USCINCSpace. These actions are undertaken in support of JTF-CND operations or coordination and do not require USCINCSpace coordination or approval. This does not preclude the staffs briefing or informing the CINC or Deputy CINC of these actions during routine operations updates or for situational awareness purposes.

l. Actions taken or directed under the authority of CJTF in response to an intrusion or incident. Relates to CJTF authority boundaries and level of authority decisions.

m. Operations Order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation.

n. Operations Impact.

1. Impact of Event/Incident. The effect upon DoD missions and operations as a result of a direct or indirect computer network event or incident. Relates to CJTF authority boundaries and level of authority decisions.

2. Impact of JTF-CND Directed Actions/Response. The effect upon DoD missions and operations as a result of the response actions directed by the CJTF. Relates to CJTF authority boundaries and level of authority decisions.

o. Space Operations Center (SPOC). SPOC CND Watch Officer/Watch NCO (CWO/NCO). Crew duty position within 24x7 operations center responsible for real-time operations within 24 hours. SPOC watch Officer is the USSPACECOM counterpart to the JTF-CND watch Officer (JTF WO). The SPOC Future Operations Branch (FOB) is responsible for operations planning from 24 hours to 72 hours.

p. Tactical Control (TACON). TACON is defined by Joint Publication (JP) I-02 as: 'Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and usually local direction and control of movements or maneuvers necessary to accomplish assigned missions or tasks. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at, any level at or below the level of combatant command."

q. Thresholds. Boundary conditions or level of authority lines used by CJTF to determine the requirements of when to seek USCINCSpace approval or direction.

r. Watch Officer/Watch NCO (CWO/NCO). See SPOC above.

Appendix D - GLOSSARY

Acronyms and Abbreviations

AAR	After Action Review
AFSCN	Air Force Satellite Control Network
AUTODIN	Automatic Digital Network
B/P/C/S	Base, Post, Camp, Station
BS	Battle Staff
CAAP	Critical Asset Assurance Program
CAT	Crisis Action Team
C2AS	
CERT	Computer Emergency Response Team
CI	Counter Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CINCSPACE	Commander in Chief, Space
CIP	Critical Infrastructure Program
CIRT	Computer Information Response Team (Navy version of CERT)
CJCS	Chairman, Joint Chiefs of Staff
CJTF-CND	Commander, Joint Task Force, Computer Network Defense
CMOC	Cheyenne Mountain Operations Center
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COA	Course of Action
COCOM	Combatant Command
COMPUSEC	Computer Security
COMAFFOR	Commander, Air Force Forces
COMARFOR	Commander, Army Forces
COMMARFOR	Commander, Marine Corps Forces
COMNAVFOR	Commander, Navy Forces
CONPLAN	Contingency Plan
CONOPS	Concept of Operations
COP	Common Operating Picture
COSIN	Controllers Instruction
CMP	Collection Management Plan
CNCO	CND Watch NCO (SPOC)
CRC	Crisis Response Cell
C/S/A	CINCs, Services and Agencies
CWO	CND Watch Officer (SPOC)
DIAP	Defense-wide Information Assurance Program
DII	Defense Information Infrastructure

DIO	Defense Information Operations
DIOP	Defense Information Operations Process
DIRLAUTH	Direct Liaison Authority
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DOR	Daily Operations Report
DSCS	Defense Satellite Communication System
DRSN	Defense Red Switch Network
EEI	Essential Element of Information
EMAIL	Electronic Mail
FOB	Future Operations Branch
FRAGO	Fragmentation Order
GCCS	Global Command and Control System
GNIE	Global Networked Information Enterprise
GNOSC	Global Network Operations Security Center
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
IO	Information Operations
IPL	Integrated Priority List
INFOSEC	Information Security
INFOCON	Information Control
ITWAA	Intelligence, Tactical Warning and Assessment
I&W	Indication and Warning
JCS	Joint Chiefs of Staff
JEKG	Joint Exercise Control Group
JIOC	Joint Information Operations Center
JMETL	Joint Mission Essential Task List
JMRR	Joint Monthly Readiness Review
JOPES	Joint Operational Planning and Execution System
JROC	Joint Requirements Oversight Committee
JSCP	Joint Strategic Capabilities Plan
JTF-CND	Joint Task Force, Computer Network Defense
JTP	Joint Training Plan
JULLS	Joint Universal Lessons Learned System
JWCA	Joint Warfare Capability Analysis
JWICS	Joint Worldwide Intelligence Communication System
JWRAC	Joint Web Risk Assessment Cell

LEA	Law Enforcement Agency
LNO	Liaison Officer
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Event Scenario List
NCA	National Command Authority
NIPERNET	Internet Protocol Router Network
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
OCS	Odyssey Collaboration System
OPLAN	Operations Plan
OPREP	Operations Report
OPSEC	Operations Security
PIR	Priority Intelligence Requirement
PBX	
PDAS	Planning Decision and Aid System
PDM	Presidential Decision Memorandum
POM	Program Objective Memorandum
PPD	Plans, Policy and Doctrine
RAP	Remedial Action Product
RSOI	Reception, Staging, Onward movement and Integration
SAV	Staff Assistance Visits
SROE	Standing Rules of Engagement
SIPERNET	Secret Internet Protocol Router Network
SITREP	Situation Report
TA	Trusted Agent
TACON	Tactical Control
TTP	Tactics, Techniques and Procedures
UCP	Unified Command Plan
UI	Unified Instructions
VTC	Video Teleconference
WNCO	Watch Noncommissioned Officer
w o	Watch Officer